



Australian Government

Australian Institute of Criminology

The Australian Business Assessment of Computer User Security: a national survey

Kelly Richards

AIC Reports
Research and
Public Policy Series

102

The Australian Business Assessment of Computer User Security: a national survey

Kelly Richards

AIC Reports

Research and
Public Policy Series

102

www.aic.gov.au



© Australian Institute of Criminology 2009

ISSN 1836-2060 (Print)

1836-2079 (Online)

ISBN 978 1 921532 34 4 (Print)

978 1 921532 35 1 (Online)

Apart from any fair dealing for the purpose of private study, research, criticism or review, as permitted under the *Copyright Act 1968* (Cth), no part of this publication may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Inquiries should be addressed to the publisher.

Project no. 0133

Ethics approval no. PO114

Dataset no. 0105

Published by the Australian Institute of Criminology

GPO Box 2944

Canberra ACT 2601

Tel: (02) 6260 9200

Fax: (02) 6260 9299

Email: front.desk@aic.gov.au

Website: <http://www.aic.gov.au>

Please note: minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at <http://www.aic.gov.au>

Foreword

As information and communication technologies have become integral to everyday life, new crimes and criminal opportunities have emerged that present risks to households, individuals, the government and the economy. It is important to understand these risks, as well as the efficacy of legislative and policy responses, and the security measures aimed at preventing and detecting computer security incidents.

This report presents the main findings from the first large scale survey of businesses in Australia about the nature and extent of computer security incidents. Although there has been some effort to research and document the risks to businesses in Australia and overseas, this national survey of businesses represents the most comprehensive assessment in Australia on computer security incidents and their prevention to date. The survey found that, based on responses from 4,000 businesses ranging in both size and industry sector, more than one in 10 (14%) businesses had experienced one or more computer security incidents during the 2006–07 financial year. The most common type of incident experienced was a virus or other malware code and the most common effect was corruption of hardware and software. The total financial loss as a result of computer security incidents against businesses in Australia during the 2006–07 financial year was estimated at between \$595 and \$649 million.

Most businesses dealt with incidents internally, with only eight percent reporting the most significant incident to police. This was primarily because victimised businesses believed the incident was not serious enough to warrant reporting it to police. The annual cost of protection against computer security incidents for Australian businesses was estimated to be \$1.37 to \$1.95 billion. Most businesses reported using one or more computer security tools and the

most common tool was anti-virus software. Nearly half of surveyed businesses had one or more security policies in place and during the 2006–07 financial year, one-quarter had undertaken an evaluation of their security.

The size of a business is an important factor that impacts on levels of reported victimisation, its cost and the cost of security measures. Large businesses were more likely to report experiencing security incidents and greater mean losses (an average of \$49,246 per business experiencing a computer security incident during 2006–07). However, large businesses also reported having more comprehensive security measures, with nearly all reporting the use of one or more security tools and the use of one or more security policies. Additionally, the mean computer security expenditure of large businesses was over 38 times that of small businesses. This indicates that large businesses are in a better position to detect incidents, but they may also require greater security as they could be subject to more serious incidents. More than twice the number of large businesses had reported their most serious security incident to police compared with small businesses.

There were few differences by industry sector, with the prevalence and type of incidents experienced being fairly consistent across industry sectors. However, there were differences in mean losses and the use of security tools and policies across sectors.

Taken as a whole, results from the Australian Business Assessment of Computer User Security (ABACUS) survey will act as crucial baseline information that can be used, through similar surveys undertaken in the future, to examine trends in victimisation and protection measures. Importantly, the results highlight how prevention policies and strategies need to involve partnerships between

government and the private sector, as many information and communication technology security measures are currently provided by the private sector and the overwhelming majority of detected incidents are handled internally by businesses.

Although it seems the risk to businesses of computer security incidents is spread broadly across business irrespective of size and sector,

the capacity of small and medium businesses to prevent and detect such incidents is not as great and they may be less aware of, and therefore more vulnerable to, the more serious crime implications associated with computer security incidents.

Dr Judy Putt
General Manager, Research

Contents

iii	Foreword	
ix	Acknowledgements	
x	Acronyms	
xi	Executive summary	
xi	Prevalence of computer security incidents	
xi	Nature of computer security incidents	
xii	Effects of computer security incidents	
xii	Responding to computer security incidents	
xii	Use of computer security tools and policies	
xiii	Expenditure on computer security measures	
xiii	Evaluation of computer security measures	
xiii	Outsourcing of computer security measures	
xiv	Implications of findings	
1	Introduction	
1	The project	
2	Defining cybercrime	
3	The Australian legislative framework	
3	Why is computer security for businesses important?	
4	Are businesses concerned about computer security incidents?	
4	What do we know about computer security incidents against businesses?	
5	What other research has been conducted on computer security incidents against businesses?	
7	A note on comparing survey data	
8	Definitions	
8	Sampling	
9	Reference periods	
9	Weighted versus unweighted data	
9	How does ABACUS differ from existing surveys on computer security incidents against businesses?	
11	Respondents in the ABACUS survey	
11	The respondents	
14	Respondents' roles within businesses	
14	Respondents' knowledge of and ability to use information technology	
15	Businesses' use of information technology	
16	Expenditure on information technology	
17	Preventing computer security incidents against Australian businesses	
17	Businesses' use of computer security tools	
19	Physical computer security tools	
19	Cryptographic and authentication tools	
21	Anti-fraud and malware computer security tools	
22	Detection and monitoring computer security tools	
23	Security management computer security tools	
25	Key findings on businesses' use of computer security tools	
27	Businesses' use of computer security policies	
28	Staff/user-related computer security policies	
30	Security testing computer security policies	
31	Data related computer security policies	
32	Incident response computer security policies	
33	External business computer security policies	
34	Wireless computer security policies	
35	Key findings on businesses' use of computer security policies	
36	Businesses' use of information technology standards	
37	Expenditure on computer security	
40	Expenditure on computer security tools	
42	Evaluation of computer security	

43	Outsourcing	83	Conclusion
46	Insuring against computer security incidents	83	Summary of key findings
47	Computer security awareness-raising initiatives	84	Some implications of key ABACUS findings
49	Prevalence of computer security incidents against Australian businesses	88	Future research directions
49	Number of computer security incidents experienced	89	References
52	Which business types are more likely to experience computer security incidents?	92	Appendix 1: Methodology
52	Business size and likelihood of experiencing computer security incidents	92	Sampling
53	Industry sector and likelihood of experiencing computer security incidents	92	The survey instrument
55	Expenditure on computer security and number of computer security incidents experienced	93	The pilot study
56	Businesses' e-literacy and number of computer security incidents experienced	94	Main data collection
58	Nature of computer security incidents against Australian businesses	94	Initial telephone call
58	Types of computer security incidents experienced	94	Initial mail-out
61	Types of computer security incidents experienced by industry sectors	94	Telephone follow-up
62	Computer security incidents originating from within businesses	95	Questionnaire re-mailing
64	Computer security incidents causing greatest financial loss	95	Response rates
66	Most significant computer security incidents experienced by businesses	95	Weighting of data
68	Effects of computer security incidents against Australian businesses	96	Appendix 2: Glossary
68	Effects of computer security incidents against businesses	96	Types of information technologies
69	Financial losses resulting from computer security incidents	96	Types of computer security incidents
75	Responding to computer security incidents against Australian businesses	97	Computer security incident outcomes
75	Reporting computer security incidents against Australian businesses	98	Computer security measures
79	Satisfaction with reporting of computer security incidents	100	Computer security policies
80	Businesses' reasons for not reporting computer security incidents	101	External business policies
		102	Computer security and outsourcing evaluation methods
			Figures
		15	Figure 1: Use of information technology, by business size
		18	Figure 2: Businesses' use of computer security tools, by industry sector
		19	Figure 3: Businesses' use of physical computer security tools, by business size
		20	Figure 4: Businesses' use of cryptographic and authentication tools, by business size
		22	Figure 5: Businesses' use of anti-fraud and malware tools, by business size
		23	Figure 6: Businesses' use of detection and monitoring tools, by business size

27	Table 10: Use of computer security policies, by business size	54	Table 30: Number of computer security incidents experienced, by industry sector
36	Table 11: Use of information technology standards in the development of computer security policies, by business size	56	Table 31: Expenditure on information technology security by number of computer security incidents
37	Table 12: Total information technology security expenditure, by business size	57	Table 32: Respondents' knowledge of, and ability to use, information technology, by number of computer security incidents experienced
38	Table 13: Estimated total information technology security expenditure across all Australian businesses	63	Table 33: Computer security incidents originating from within, by business size
39	Table 14: Total information technology security expenditure, by industry sector	66	Table 34: Computer security incident causing greatest financial loss, by business size
39	Table 15: Estimated total information technology security expenditure across all Australian businesses, by industry sector	67	Table 35: Most significant computer security incident, by business size
40	Table 16: Expenditure on physical computer security	69	Table 36: Impacts experienced as a result of most significant computer security incident, by business size
41	Table 17: Expenditure on cryptographic and authentication tools	70	Table 37: Estimated financial losses from all computer security incidents, by business size
41	Table 18: Expenditure on anti-fraud and malware tools	71	Table 38: Estimated financial losses from all computer security incidents across Australian businesses
41	Table 19: Expenditure on detection and monitoring tools	72	Table 39: Estimated financial losses from all computer security incidents, by sector
42	Table 20: Expenditure on security management tools	72	Table 40: Estimated financial losses from all computer security incidents across businesses experiencing computer security incidents, by sector
42	Table 21: Method of evaluation of computer security, by business size	73	Table 41: Estimated financial losses from computer security incidents across all Australian businesses, by sector
43	Table 22: Frequency of evaluation of computer security measures, by business size	74	Table 42: Respondents' knowledge of, and ability to use, information technology, by total cost of computer security incidents
44	Table 23: Outsourcing of computer security measures, by business size	80	Table 43: Victimised businesses' reasons for not reporting most significant computer security incident to an external party, by business size
44	Table 24: Offshoring of computer security measures, by business size	93	Table 44: Sample selections by industry sector and business size
45	Table 25: Method of evaluation of outsourced computer security, by business size	95	Table 45: Response rate by industry sector and business size
45	Table 26: Frequency of evaluation of outsourced computer security measures, by business size		
47	Table 27: Computer security incidents covered by insurance policies, by business size		
48	Table 28: Familiarity with awareness-raising initiatives, by business size		
53	Table 29: Annual turnover, by number of computer security incidents experienced		

Acknowledgements

The research reported in this paper was funded under the *Proceeds of Crime Act 2002*, which is administered by the Australian Government Attorney-General's Department

This research would not have been possible without the cooperation of respondents from small, medium and large businesses across Australia. Their time and effort in completing the ABACUS survey is greatly appreciated.

The input of stakeholders, including members of the Business and Technical Advisory Groups is also much appreciated. The considerable expertise they contributed to the research is acknowledged.

The hard work, support and assistance of the Social Research Centre, who were responsible for the project's data collection, assistance with the survey

design and cleaning and coding of the data, as well as having substantial input into the overall direction of the ABACUS project, is also greatly appreciated.

Russell Smith, the AIC's Principal Criminologist, has been involved in the ABACUS project throughout all its stages and has made invaluable contributions to its design, implementation and direction. The input of Rachelle Irving into the developmental stages of the project is also acknowledged.

The author would also like to thank Natalie Taylor and Judy Putt for their input, guidance and support throughout the project and Jason Payne for his considerable input into the cleaning and coding of the statistical data that the ABACUS study generated, and his assistance with data analysis.

Acronyms

ABACUS	The Australian Business Assessment of Computer User Security
ABR	Australian Business Register
ABS	Australian Bureau of Statistics
AIC	Australian Institute of Criminology
ANZSIC	Australian and New Zealand Standard Industrial Classification
AusCERT	Australian Computer Emergency Response Team
CATI	Computer-assisted telephone interview
ICT	Information and communication technologies
ISP	Internet Service Provider
SRC	Social Research Centre
TISN	Trusted Information Sharing Network

Executive summary

The Australian economy relies on networked computer systems across all business sectors to facilitate service delivery and communication between government, the private sector and the general public.

The Australian Institute of Criminology (AIC) undertook a survey of small, medium and large businesses from a range of industry sectors and from all Australian states and territories during February – April 2008 regarding the prevalence and nature of computer security incidents they had experienced, the areas in which business systems are vulnerable to such incidents and the cost, types and effectiveness of approaches Australian businesses use to prevent them. In total, 4,000 businesses completed the ABACUS questionnaire, representing a response rate of 29 percent. The findings of this research, presented in this report, may be used by businesses in Australia to assess the effectiveness of their information technology security measures and to inform improvements to these measures in the future.

Prevalence of computer security incidents

- Fourteen percent of businesses with information technology experienced one or more computer security incidents during the 12-month period from 1 July 2006 to 30 June 2007. Twelve percent experienced one to five incidents; one percent, six to 10 incidents; and one percent, more than 10 incidents.
- Large businesses experienced more computer security incidents than medium businesses, and medium businesses experienced more computer security incidents than small businesses.
- A greater proportion of businesses with a high annual turnover experienced computer security incidents than did those with a low annual turnover.
- The proportion of businesses experiencing computer security incidents was found to be quite even across industry sectors. The proportion of businesses reporting no incidents ranged from 70 percent of financial and insurance services businesses to 85 percent of businesses belonging to the other services category.
- The proportion of businesses in the ABACUS survey that experienced computer security incidents was similar to that found in previous research on Australian businesses. The proportion is much lower, however, than that found in US research.

Nature of computer security incidents

- The computer security incident experienced by the highest proportion of victimised businesses was a virus or other malicious code. Sixty-four percent of businesses that were victimised by one or more computer security incidents (65% of small, 61% of medium, 52% of large businesses) experienced this type of attack.
- Eleven percent of victimised businesses experienced one or more computer security incidents originating from within their organisation. This is a smaller proportion of businesses than has been found by previous surveys on computer security incidents against businesses.

- Viruses and other malicious code were ranked as the most significant computer security incident by the highest proportion of victimised businesses (54%). Small (57%) and medium (39%) businesses were most likely to report viruses or malicious code as their most significant incident. Large businesses (24%) were most likely to rate theft or loss of hardware as their most significant incident.
- Similar proportions of businesses in each industry sector experienced each type of computer security incident. Viruses or other malicious code was the type of computer security incident most commonly experienced by businesses in each industry sector.
- Among those that had experienced one or more incidents, the manufacturing sector reported the highest mean losses due to computer security incidents (\$13,295), followed by the retail sector (\$9,870). The lowest mean losses were reported by businesses in the agricultural, forestry and fishing sector (\$1,155).
- Total losses due to computer security incidents against all Australian businesses in 2006–07 have been estimated at between \$595m and \$649m.

Effects of computer security incidents

- Seventy-seven percent of businesses (75% of small, 88% of medium, 95% of large businesses) that had been victimised by one or more computer security incident experienced some type of negative effect following their most significant computer security incident.
- The most common effect experienced was corruption of hardware or software, with 40 percent of victimised businesses experiencing this type of outcome. Forty-two percent of small, 35 percent of medium and 31 percent of large businesses reported corruption of hardware or software following their most significant computer security incident.
- Small (42%) and medium (35%) businesses were most likely to experience corruption of hardware or software as a result of their most significant computer security incident. Large businesses (40%) were most likely to report theft or loss of hardware, followed by unavailability of service (39%).
- Across businesses that experienced at least one computer security incident, the mean loss due to computer security incidents during the 2006–07 financial year was \$4,469. For small businesses, the mean loss was \$2,431; for medium businesses, \$12,405; for large businesses, \$49,246.
- The most common response by businesses to their most significant computer security incident was to deal with it internally. Seventy-seven percent of businesses (78% of small, 74% of medium, 72% of large businesses) that experienced a computer security incident reported this response.
- Only eight percent of victimised businesses (7% of small, 14% medium, 21% large businesses) reported their most significant computer security incident to the police. This closely reflects previous research on computer security incidents against businesses that was undertaken by the Australian Bureau of Statistics (ABS), but departs considerably from the findings of other Australian and international research.
- The most common reason given for not reporting their most significant computer security incidents was that the incident was not serious enough to report. Forty-eight percent of victimised businesses (49% of small, 43% of medium, 27% of large businesses) identified this as one of the reasons they chose not to report their most significant computer security incident to an external agency.

Responding to computer security incidents

- The most common response by businesses to their most significant computer security incident was to deal with it internally. Seventy-seven percent of businesses (78% of small, 74% of medium, 72% of large businesses) that experienced a computer security incident reported this response.
- Only eight percent of victimised businesses (7% of small, 14% medium, 21% large businesses) reported their most significant computer security incident to the police. This closely reflects previous research on computer security incidents against businesses that was undertaken by the Australian Bureau of Statistics (ABS), but departs considerably from the findings of other Australian and international research.
- The most common reason given for not reporting their most significant computer security incidents was that the incident was not serious enough to report. Forty-eight percent of victimised businesses (49% of small, 43% of medium, 27% of large businesses) identified this as one of the reasons they chose not to report their most significant computer security incident to an external agency.

Use of computer security tools and policies

- Eighty-five percent of businesses (84% of small, 93% of medium, 96% of large businesses) that used information technology reported using one or more computer security tools.

- The most commonly used type of computer security tool was anti-virus software. Eighty-five percent of businesses (84% of small and 91% of both medium and large businesses) reported using this type of computer security tool.
- Use of computer security tools by sector ranged from 79 percent of construction sector businesses to 92 percent of businesses in education and training and in financial and insurance services.
- Forty-two percent of businesses (38% of small, 72% of medium, 90% of large businesses) with information technology reported using one or more computer security policies.
- Media backup policies were the most commonly used computer security policy. Thirty percent of businesses (26% of small, 55% of medium, 82% of large businesses) reported using this type of policy.
- The education and training sector reported the highest use of computer security policies, with 57 percent of businesses in this sector using one or more policies. The industry sector reporting the lowest level of computer security policy use was agriculture, forestry and fishing at 26 percent.
- A smaller proportion of businesses reported using almost all computer security tools and policies than has been found in previous surveys in Australia and overseas.

Expenditure on computer security measures

- The mean information technology security expenditure for businesses during the 12-month period from 1 July 2006 to 30 June 2007 was \$1,830 (small businesses, \$992; medium businesses, \$7,614; large businesses, \$38,474).
- The total computer security expenditure for all Australian businesses for the period has been estimated at between \$1.37b and \$1.95b.

Evaluation of computer security measures

- Twenty-four percent of businesses that used computer security measures evaluated their computer security during the 2006–07 financial year.
- The most commonly used method of evaluation was a security audit by an internal staff member. In total, 32 percent of businesses used this method.
- Small businesses (30%) were most likely to use security audits by internal staff and/or email monitoring software to evaluate their computer security. Medium businesses (40%) were most likely to use security audits by internal staff. Large businesses were most likely to use email monitoring software (53%), followed closely by security audits by internal staff (52%).

Outsourcing of computer security measures

- Nineteen percent of businesses (17% of small, 38% of medium, 42% of large businesses) with information technology outsourced one or more computer security functions to a third party.
- Fifteen percent of those businesses (15% of small, 11% of medium, 31% of large businesses) outsourced computer security functions to a third party based outside of Australia.
- A smaller proportion of ABACUS respondents reported outsourcing computer security measures than previous surveys have shown.

Implications of findings

- Currently, law enforcement agencies appear to play a marginal role in policing and/or responding to computer security incidents against businesses. If reporting is to increase, it is important for legislators, policymakers and law enforcement agencies to be aware of the various costs associated with reporting computer security incidents (including temporal and financial) and to implement strategies to reduce them.
- The types of computer security incidents that may facilitate the theft of personal data were experienced by a large proportion of businesses. Legislators, policymakers and law enforcement agencies should be aware that such computer security incidents may lead to the commission of more serious crimes. Strategies to determine the extent of this problem and to minimise these types of offences are therefore critical.
- The ABACUS data suggest that cyber criminals appear to be mostly opportunistic offenders. That is, the types of attacks experienced most frequently by businesses are usually indiscriminate. A focus on minimising the opportunities for cyber criminals, raising awareness among businesses and to have businesses improve and increase their use of computer security tools and policies is therefore important.



Introduction

Information and communication technologies (ICT) have become an integral part of the functioning of modern societies around the world, particularly in western society. An increasing proportion of internet users in Australia now use an internet connection with a high bandwidth (Australian Communications and Media Authority 2008; Australian Computer Emergency Response Team (AusCERT) 2008: 7). Developed nations, such as Australia, now rely heavily on networked computers for a range of important functions (Australian Communications and Media Authority 2007), including communications and financial and energy services (Jones 2007: 602).

According to the ABS, the majority of Australian businesses report both computer use (89%) and internet use (81%; ABS 2007: 4). Of those businesses with internet access, the majority (83%) report using a broadband connection. Businesses report using the internet for a variety of functions, including online banking and other financial activities enabling persons to work from home or other locations, and gathering information related to the business's products and/or services (ABS 2007: 15).

The increasing use of, and reliance on, ICT has resulted in a variety of new crimes and opportunities for existing crimes (such as fraud) to be committed in new ways via such technology (Jones 2007: 602; Smith 2007: 167). There has been a substantial increase in the reported costs of cybercrimes

(Rollings 2008) and a range of terms such as 'cyberstalking', 'cyberbullying', 'spamming', 'phishing' and 'identity theft' have entered the public discourse. (for further discussion of definitions see AIC 2006a, 2006b, 2005. A full glossary of terms used in the ABACUS project is included at Appendix 3).

The emergence of these new crimes, or at least new methods for committing crimes, has prompted a large body of literature and research on cybercrimes. Overviews of this literature (see Choo, Smith & McCusker 2007a; Urbas & Choo 2008) are a useful resource in developing an understanding of cybercrime and the complex concerns arising from the commission, policing, prevention, detection and prosecution of these offences. This report, however, focuses specifically on computer security incidents against businesses.

The project

The ABACUS project involved undertaking a nationwide survey of small, medium and large businesses from all industry sectors on their experiences of cybercrime. Businesses were asked to complete a questionnaire about the measures they had taken during the 2006–07 financial year to protect their computer systems, the number and

type of computer security incidents they experienced, the impacts of these incidents and how they responded to computer security incidents. Key stakeholders were involved in the design of the questionnaire. A copy of the questionnaire is included with the Technical and Background Paper on the ABACUS study (see Challice 2008). A summary of the study's methodology is included in Appendix 1.

This report presents the findings from the ABACUS survey on computer security incidents against businesses. These findings are compared throughout with the results of other surveys that have previously been undertaken in Australia and overseas on computer security incidents against businesses.

Defining cybercrime

The use of complex terminology is unavoidable in research on computer security incidents. Definitions of computer-related terms will be provided as they appear throughout this report. A full glossary of terms is also included at Appendix 2.

There has been a great deal of debate on how to define 'cybercrime' (Wall 2007: 185). A number of terms are used interchangeably to describe the phenomenon of cybercrime, including virtual, online, digital, high-tech, computer-related, internet-related, telecommunications-related, computer-assisted, electronic, ICT-related and e-crime (Choo, Smith & McCusker 2007a: 2; Smith, Grabosky & Urbas 2004: 5). Many researchers attempt to make sense of what constitutes a cybercrime—or at least construct some parameters around this term—by grouping these offences into categories. Typically, cybercrimes are categorised according to whether they are 'computer-assisted' or 'computer-focused' (Yar 2005: 409–10); that is, whether a crime is *enabled* by a computer, or simply *enhanced* by the use of a computer (Grabosky 2007: 202). Computer *enhanced* offences are those in which computers make it easier to commit an offence; computer *enabled* offences are those in which a computer is required for the commission of the offence (Choo, Smith & McCusker 2007a: 2). In addition to using computers *in the commission* of offences,

cybercrimes can also be *directed at* computing technologies themselves (Smith, Grabosky & Urbas 2004: 7). Computers may also be incidental to the commission of other crimes (Smith, Grabosky & Urbas 2004: 7). See Brenner (2007: 381–386) and Urbas and Choo (2008: 2–3) for more detailed discussions of definitional issues.

The ABACUS study focuses on computer enhanced and computer enabled offences against businesses. The survey uses the term 'computer security incident' rather than 'cybercrime'. The use of this term is important for two main reasons. First, its use aims to capture incidents that, although illegal, may not be considered 'crimes' by victims themselves. Second, although all 'computer security incidents' may be cybercrimes, not all cybercrimes are computer security incidents. The ABACUS survey focuses specifically on computer security incidents against businesses, rather than considering cybercrimes (such as online pornography offences or cyber stalking) more broadly. The term 'computer security incident' will be used throughout the remainder of this report.

The ABACUS survey defined a 'computer security incident' as *any unauthorised use, damage, monitoring attack or theft of your business information technology*. Incidents can therefore be considered successful security breaches rather than attempts. Respondents were instructed that each incident should only be counted once. For example, any worm or virus that could be classified as a computer security incident should only be counted as a single attack, not once per infected machine.

Previous surveys on computer security incidents against businesses have used varying terminology to describe these phenomena, including 'security breaches', 'electronic attacks' and 'security events'. Definitions also vary among these surveys. AusCERT (2006: 17) define 'electronic attacks' as those that harm 'the confidentiality, integrity or availability of network data or systems'. The Computer Emergency Response Team et al. (2007) defines a 'security event' as 'an adverse event that threatens some aspect of computer security'. In the latter survey, respondents were instructed that spam and phishing emails, virus-carrying emails and routine network or port scanning activities that are blocked by standard perimeter defences, and the discovery

of vulnerabilities in packaged software, were not to be counted as ‘security events’.

Many research reports stemming from surveys on computer security incidents against businesses do not reveal how computer security incidents were defined. Importantly, however, the types of computer security incidents that are listed (such as viruses, worms, denial of service attacks and sabotage) are very similar among these surveys, and it can be assumed that these examples inform respondents’ understanding of the topic area. The differences among definitions used in studies on computer security incidents against businesses are discussed in more detail later in this Introduction.

The Australian legislative framework

In Australia, computer security incidents are legislated against in various state, territory and Commonwealth laws. The *Cybercrime Act 2001* (Cth) came into effect on 1 October 2001. This Act added new provisions to existing Commonwealth legislation, including the *Criminal Code Act 1995* (Cth), the *Crimes Act 1914* (Cth) and the *Customs Act 1901* (Cth) (Urbas & Choo 2008: 20). The Act also influenced state and territory legislation and, with some changes, has been followed in the Australian Capital Territory, New South Wales,

the Northern Territory, Victoria and South Australia (Urbas & Choo 2008: 20–21). Table 1 outlines the current relevant legislation for each of Australia’s states and territories.

See Urbas and Choo (2008) for a detailed discussion of Commonwealth, state and territory cybercrime legislation in Australia.

Why is computer security for businesses important?

Businesses’ computer security incidents are an important research area for a variety of reasons. Perhaps most importantly, computer security incidents represent a potential threat to the ‘critical national infrastructure’. This is infrastructure that if damaged or rendered unusable, would detrimentally affect the social or economic wellbeing or security of the nation (see www.tisn.org.au). Advanced economies such as Australia rely fundamentally on networked computer systems for a range of crucial functions, including services in communication, finance, energy, transport and air-traffic control. These functions are ‘increasingly—if not exclusively—controlled by computers’ (Parliamentary Joint Committee on the Australian Crime Commission 2004: 53). As Choo, Smith and McCusker (2007b: 2) point out, private companies are responsible for the majority of critical infrastructure functions in Australia.

The online industry is also valuable to the Australia economy. Governments and the private sector promote the use of online facilities and internet based access to services. It appears, however, that the risks associated with computer security incidents have begun to have a negative impact on online commercial activities. For example, the ABS (2007: 26) reports that fears about computer security incidents have prevented a small percentage of businesses from providing online shopping. Similarly, Gartner analysts (cited in McAfee 2007: 19) found that one-third of online shoppers buy fewer items as a result of security fears. CyberSource (2008: 5) found that such fears prevent a small percentage of consumers from accessing online shopping websites (see also Webroot Software 2008a: 1). Eighty-two percent of surveyed consumers claim

Table 1 Main computer-related offence legislation		
Act	Relevant section(s)	
ACT	<i>Criminal Code 2002</i>	ss 415–421 and s 423
NSW	<i>Crimes Act 1900</i>	ss 308C–308I
NT	<i>Criminal Code Act</i>	ss 276B–276E
Qld	<i>Criminal Code Act 1899</i>	s 408E
SA	<i>Summary Offences Act 1953</i>	s 44 and s 44A
	<i>Criminal Law Consolidation Act 1935</i> (Part 4A)	ss 86E–86H
Tas	<i>Criminal Code Act 1924</i>	ss 257B–257E
	<i>Police Offences Act 1935</i>	ss 43A43D
Vic	<i>Crime Act 1958</i>	ss 247B–247H and ss 247K–247L
WA	<i>Criminal Code</i>	ss 440A(3)(a)–440A(3)(c)

Source: adapted from Urbas and Choo (2008)

they will only shop online with large, well-known retailers, which CyberSource acknowledge is 'worrying...for new businesses' (Cybersource 2005: 19) and thus for the economy more generally. Computer security incidents against businesses are therefore thought to represent 'the dark side of a free-flowing, dynamic informational economy' (Marron 2008: 22).

Previous research studies on computer security incidents against businesses have shown that these can be very costly for businesses. Although it is difficult to accurately determine the cost of computer security incidents against businesses, a number of previous surveys have asked business respondents to estimate the losses they have suffered due to incidents of this nature. AusCERT (2006: 26) found that the total average annual loss for businesses was \$241,150. Richardson's (2007: 16) research in the United States found that the average loss per business respondent was US\$345,000. Other US research (Computer Emergency Response Team et al. 2006) reported higher losses again, with an average loss per business of US\$465,700. Quinn's (2006: 11) study of businesses in New Zealand found that the average cost per computer security incident was NZ\$3,000. The Department of Trade and Industry's (2007: 30) research in the United Kingdom found an average cost to business of £8,000–17,000 for their worst computer security incident. Rantala's (2008: 1) research estimated that financial losses resulting from computer security incidents against businesses in the United States during 2005 were US\$867m. Although these studies employed varying research methodologies and must be considered with caution (as discussed in detail below), they provide an insight into the potentially devastating effects that such incidents may have on businesses.

Are businesses concerned about computer security incidents?

Businesses are concerned about the risks associated with computer security incidents and believe that victimisation is widespread (e.g. see Nykodym, Taylor & Vilela 2005: 411;

Smith, Grabosky & Urbas 2004: 14). A survey commissioned by IBM found that about half of Australian businesses perceive computer security incidents as a greater threat, and more costly to their organisation, than physical crime (Ho 2006: 9). Governments are also concerned about the threat posed by computer security incidents against businesses and the effect that they may have on the effective operation of the critical infrastructure.

Computer security incidents therefore present a significant potential threat to businesses. The importance to them of online security must be weighed up against the imperative of maximising profits by providing ease of access for consumers. Businesses occupy an awkward position as there are considerable costs associated with 'orders lost from over-zealous anti-fraud policies' (CyberSource 2008: 8).

The paucity of statistically sound research in this area, combined with a reliance on the media for relevant information and frightening reports from vendors might therefore prevent businesses from making informed decisions about how to most effectively protect information technology systems from computer security incidents (Marron 2008; Wall 2007: 184). In turn, this may leave businesses' information technology systems open to security incidents.

What do we know about computer security incidents against businesses?

Currently, we know very little about the extent, nature or effects of computer security incidents against businesses. There are a number of reasons for this. First, there is a paucity of data for researchers to draw on. This is at least partly a result of under-reporting of computer security incidents (discussed in detail later in this report). Under-reporting is, in turn, related to the lack of consensus as to what constitutes a computer security incident. The language often adopted — 'breaches' or 'security incidents' rather than 'crimes' — undoubtedly results in confusion among businesses as to whether they have been victims of 'real' crimes. As Wall (2007:

185) commented, 'although there is fairly widespread consensus that cybercrimes exist, there is much confusion as to what they actually are and what risks they pose' (see also McCusker 2006). Further, cases of reported computer security incidents rarely result in prosecutions (Allan 2005: 151) and as a result, there is little police or court data for researchers to draw on.

There is little accurate information available on the financial effect of computer security incidents against businesses due to the difficulty in quantifying losses caused by these incidents. For example, there is no reliable method for measuring company losses due to computer 'downtime' as a result of computer security incidents (Richardson 2007: 3). It is also very difficult to determine the losses businesses suffer as a result of computer security incidents, as some of these losses may be impossible to quantify. For example, stolen data are extremely difficult to place a dollar value on (see Nykodym, Taylor & Vilela 2005: 411). Finally, evidence of computer security incidents is highly sensitive information to the business affected. Knowledge that a business has experienced computer security breaches may render the business vulnerable to further breaches and may result in reduced confidence by consumers and therefore reduced profit or sales.

These factors combined render computer security incidents against businesses an unwieldy topic area for researchers. Nonetheless, a small body of research literature on the topic has emerged in recent years. This is summarised below.

What other research has been conducted on computer security incidents against businesses?

A number of studies around the world have considered the phenomenon of computer security incidents against businesses. Research studies that have gathered data that is comparable with the ABACUS study are used as a point of comparison and explored in more detail in this report (ABS 2007; AusCERT 2006; Broadhurst et al. 2006; Computer

Emergency Response Team et al. 2007; Deloitte Touche Tohmatsu 2007; Department of Trade and Industry 2006; Quinn 2006; Rantala 2008; Richardson 2007). They are outlined briefly below. Table 2 summarises the previous surveys that have been conducted in this field, including their geographical scope and the numbers and types of businesses sampled.

Australia

The AIC's ABACUS study is the first large-scale national study on computer security incidents against businesses in Australia. Prior to this, AusCERT conducted an annual survey, collecting trend data on computer security incidents against businesses. Their most recent survey was conducted in 2006. As Table 2 shows, AusCERT sampled 389 businesses in their most recent survey. Prior to this, the sample size was smaller again.

The ABACUS study builds on AusCERT's previous work by surveying a larger sample of Australian businesses. As discussed below, the ABACUS study's representative sample of Australian businesses allows conclusions to be drawn about the broader Australian business population.

The ABS *Business Use of Information Technology* survey, which aimed to assess Australian businesses' use of information technology and associated activities, asked business respondents a small number of questions in relation to computer security (ABS 2007). These questions focused on the type of information technology security measures businesses use, whether businesses had experienced an information technology security breach, and actions taken following a security breach. Although the focus of this survey was businesses' use of information technology more broadly, the ABS used a large sample of approximately 8,800 large businesses (those with 200 or more employees). Some meaningful comparisons can therefore be made between data from this survey and the ABACUS data.

New Zealand

The New Zealand *Computer Crime and Security* survey has been conducted annually since 2005

by the University of Otago's Security Research Group, in partnership with a variety of related organisations. The most recent survey explored the computer security of New Zealand businesses, including the types of computer security incidents experienced, methods of preventing computer security incidents, and responses to incidents (Quinn 2006). This survey used a very small sample of businesses (n=113) drawn from the top 500 New Zealand businesses by annual turnover and from a list of local and national government organisations (see Table 2).

Publication of results from the 2007 survey has been delayed and a report is not available at the time of writing.

Hong Kong

The Hong Kong component of the *International Crime Victim Survey* and *International Crime Against Businesses Survey* included a number of questions relating to individuals' and businesses' computer usage and 'crime victimization in cyber space'. Specifically, the survey results focus on the prevalence of computer security incidents against businesses and the reporting behaviours of businesses that experienced incidents (see Broadhurst et al. 2006).

Details of the methodology of this research have not been made publicly available. Comparisons between the results of the Hong Kong survey and the ABACUS survey must therefore be interpreted with particular caution.

Table 2 Previous surveys on computer security incidents against businesses				
	Reference period	Geographical scope	Sample size	Sample type
AusCERT	2006	Australia	389	Sample of public and private sector businesses and targeted industry groups, including the TISN
ABS	Financial year 2005–06	Australia	Approximately 8,500	Random, stratified sample of 8,800 businesses with 200 or more employees. Government/defence organisations, and those from the education and agriculture, forestry and fishing sectors, were excluded
New Zealand	2006	New Zealand	113	Sample of 500 businesses drawn from a list of top 500 businesses by annual turnover, and a list of government organisations
Hong Kong	Unknown	Hong Kong	Unknown	Unknown
United Kingdom	2006	United Kingdom	1,001	Random sample from a register of UK businesses, excluding sole traders and including a boosted sample of large businesses
Rantala (US)	2005	United States	7,818	Stratified, random sample of businesses belonging to 36 industry sectors belonging to the North American Industrial Classification System. Sole traders were excluded
CERT (US)	Financial year 2006–07	United States	671	Sampled readers of <i>Chief Security Officer</i> magazine and the US Secret Service's Electronic Crime Task Forces
CSI (US)	2006	United States	494	Sampled information security practitioners from a range of corporations
Deloitte Touche Tohmatsu	2007	Businesses with a global presence	169	Sampled information technology security specialists from major financial organisations in 32 countries

a: Deloitte Touche Tohmatsu's survey included businesses with a worldwide presence and a head office in one of the following geographic regions: Asia Pacific (excluding Japan), Japan, Former Soviet Republics—Commonwealth of Independent States, Europe, the Middle East and Africa, Canada, USA and Latin America and the Caribbean.

United Kingdom

The UK's Department of Trade and Industry commissions accounting firm PriceWaterhouseCoopers to conduct an annual survey on computer security incidents against businesses in the United Kingdom. The most recent survey collected data from 1,001 randomly-selected businesses on experiences of computer security incidents, attitudes to and awareness of information security and approaches taken to preventing and responding to computer security incidents (Department of Trade and Industry 2006). This survey's design included using a boosted sample of large businesses to allow for detailed analysis of these organisations. The Department of Trade and Industry's comparisons of large businesses with businesses overall are useful as they are able to indicate whether business size is a factor in each of the survey's findings. These can be compared with findings from the ABACUS survey.

United States

There are three major sources of data on computer security incidents against businesses in the United States: the Bureau of Justice Statistics' *Computer Security Survey* (Rantala 2008), the Computer Security Institute's *Computer Crime and Security Survey* (Richardson 2007) and the Computer Emergency Response Team et al. (2007) *E-Crime Watch Survey*.

Results from the Bureau of Justice Statistics 2005 nationwide study on computer security incidents against businesses were recently published (Rantala 2008). This survey perhaps most closely resembles the ABACUS survey, due to its large sample size and stratified, random-sample technique. The Bureau of Justice Statistics' survey yielded 7,818 responses in total.

The Computer Security Institute's annual *Computer Crime and Security Survey* is the longest-running survey in the field (Richardson 2007: 1) and has been drawn on in the development of both AusCERT's and Quinn's respective surveys on computer security incidents against businesses. Like these studies, it annually surveys a small number of businesses in relation to their experiences with preventing, experiencing and responding to

computer security incidents. The most recent study surveyed 494 information security practitioners from businesses, government agencies, financial institutions, medical institutions and universities (see Table 2).

Since 2004, the Computer Emergency Response Team has, in partnership with a number of relevant organisations, polled security and law enforcement professionals on a range of information technology security issues. The most recent survey polled 671 organisations. This research covers similar territory to those outlined above, but focuses on respondents in the field of information technology security rather than attempting a random sample of businesses (Computer Emergency Response Team et al. 2007).

Global

Deloitte Touche Tohmatsu conducts an annual survey of major financial institutions with a global presence, with the aim of helping businesses assess the state of information technology security within their own organisation against comparable businesses around the world. The study surveys a small number of business respondents about broad topics related to computer security, including types of computer security incidents experienced and measures undertaken to ensure information technology security (see Deloitte Touche Tohmatsu 2007). As Table 2 shows, the most recent Deloitte Touche Tohmatsu study for 2007 surveyed 169 respondents.

A note on comparing survey data

As stated above, where comparable data exist, results from these surveys will be compared with ABACUS data in this report. Comparing results from diverse surveys can be problematic and this type of analysis raises a number of potential concerns. As Table 2 indicates, the methodological approaches used in studies of computer security incidents against businesses vary considerably. The differences among these studies, and implications of these differences in relation to comparing results, are outlined below.

Definitions

Definitions of 'computer security incident' vary considerably among surveys of businesses. As noted earlier, the ABACUS survey defined a computer security incident as *any unauthorised use, damage, monitoring attack or theft of your business information technology*. Previous surveys on computer security incidents against businesses have used varying terminology to describe computer security incidents, as well as varying definitions. Additionally, many research reports stemming from surveys on computer security incidents against businesses do not reveal how computer security incidents were defined.

In addition to the varying definitions of 'computer security incident' used in research on this topic, survey instruments may also have used varying definitions of particular terms. Particular computer security incidents, such as 'phishing', may have been defined in a number of different ways among these surveys. Even where matching definitions have been used, variations in the phrasing of survey questions may have affected findings. The questionnaires used in previous surveys on computer security incidents against businesses are not publicly available so it is impossible to gauge how the wording of survey questions may have impacted on responses. These issues must be taken into consideration when interpreting and comparing data from these sources.

Sampling

As Table 2 indicates, previous surveys on computer security incidents against businesses have sampled varying numbers of businesses. Often, very small sample sizes have been used. Random sampling is rarely used. These surveys therefore have not necessarily been able to produce generalisable, statistically significant data. Sampling differences among surveys may influence findings and may begin to explain some of the ABACUS survey's divergent findings discussed later in this report.

Different approaches to sample composition must also be borne in mind when comparing the results of surveys on computer security incidents against

businesses. The ABACUS survey randomly sampled small, medium and large businesses from a diverse range of industry sectors. This approach was adopted to enable the ABACUS data to be generalised to the entire Australian business population. Not all previous surveys on this topic have adopted this approach. The ABS *Business Use of Information Technology* survey sampled only businesses with 200 or more employees. Government and defence organisations, businesses from the education and the agriculture, forestry and fishing sectors, private households employing staff and religious organisations were excluded. The UK's Department of Trade and Industry excluded sole traders and intentionally over-sampled large businesses to enable more detailed comparisons between these and other businesses. Rantala's (2008) survey in the United States also excluded sole traders.

Quinn's (2006) survey sampled businesses from a list of New Zealand's top 500 businesses (by annual turnover) and a list of local and national government organisations. Deloitte Touche Tohmatsu's (2007) research focused only on major financial organisations with a global presence. Almost half the sample had an annual turnover of more than \$1b. Twenty-nine percent of Deloitte Touche Tohmatsu's respondents were from the top 100 global financial institutions, 26 percent were from the top 100 global banks, 14 percent were from the top 50 global insurance companies, and 40 percent were from top payment and processes corporations.

AusCERT's survey used a sample of public and private sector organisations, but also targeted a number of industry groups, including the TISN. As many members of the TISN are likely to be large corporations, this may have skewed AusCERT's research to include proportionately more large businesses than exist in the Australian business population. Almost half of AusCERT's respondents were from businesses with 500 or more employees, and more than three-quarters were from businesses with 100 or more employees. The survey by the Computer Emergency Response Team et al. (2007) sampled readers of *Chief Security Officer* magazine and members of the US Secret Service's Electronic Crime Task Forces only. Respondents to this survey were therefore self-selected rather than randomly

sampled. This approach may not produce an accurate picture of the prevalence of computer security incidents against businesses for a variety of reasons. Members of the 'computer security community' may have a better knowledge of computer security incidents than respondents from the broader business community, and may therefore provide information quite different from that which might have been provided by respondents from diverse business sectors. Representatives of businesses who self-select to participate in surveys about computer security incidents are potentially more likely to be those who have experienced computer security incidents. Again, this may produce skewed results.

These limitations may also apply to Richardson's (2007) research in the United States, which draws respondents primarily from members of the Computer Security Institute.

Reference periods

As Table 2 indicates, surveys on computer security incidents against businesses do not all relate to the same period. It is widely accepted that time moves especially quickly in the computer security realm. Melek (cited in Deloitte Touche Tohmatsu 2007: 1) describes the sentiment that 'a year in technology is like ten in any other industry' as an 'oft-repeated tenet'. The different time periods to which surveys on computer security incidents against businesses relate may impact their findings and contribute to differences among survey findings.

Weighted versus unweighted data

Most existing surveys on computer security incidents against businesses have not used weighted data. Only the ABACUS project and the Department of Trade and Industry's research have used weighted data. The process of weighting, described in more detail later in this report, enables survey results to more accurately represent the wider business populations through proportional adjusting

of the sample to match the population distribution. It is important to be aware of this difference when comparing the findings from these surveys.

How does ABACUS differ from existing surveys on computer security incidents against businesses?

The ABACUS study is the first nationwide survey of its kind in Australia. It used a representative sample of small, medium and large businesses from all industry sectors and weighted data to more accurately reflect the Australian business population (see Appendix 1 for a detailed description of the project's methodology). Although it draws on previous studies of computer security incidents against businesses, it departs from these by providing weighted data from a large, random, representative sample of businesses across Australia.

In some instances, the ABACUS data support very different conclusions from those of previous surveys. Given the methodological differences among these surveys, this is to be expected to some extent. Therefore, although results from previous surveys are compared with ABACUS findings throughout this report, differences among the surveys must be interpreted with caution. It must also be noted that not all existing research studies have made information on their methodological approach publicly available. Possible explanations for differences among survey results are suggested where appropriate throughout this report.

As outlined above, computer security incidents against businesses is a uniquely important area. The ABACUS survey was developed in this context, and aims to begin to address the gaps in knowledge about computer security incidents against Australian businesses. The ABACUS study aims to establish how often these sorts of crimes are committed against businesses, what types of attacks are taking place, what businesses have been doing to prevent computer security incidents and how well these existing measures are working.

Findings will enable businesses to improve their computer security

The ABACUS survey explored five broad areas of businesses' computer security incidents:

- the cost, types and effectiveness of approaches to prevent computer security incidents
- the prevalence of incidents
- the types of incidents experienced
- the effects of incidents
- how Australian businesses respond to incidents.

Respondents were asked to answer the ABACUS survey's questions in relation to the 2006–07 financial year.

Findings of the ABACUS survey, presented in this report, will enable businesses to improve their computer security, as well as allow continued safe use of online functions by consumers.

Additionally, the findings will be useful in helping Australian businesses and government agencies to effectively allocate resources to prevent computer security incidents.



Respondents in the ABACUS survey

The respondents

In total, the AIC attempted to contact 13,941 businesses and request that they complete the ABACUS survey either on paper, online or on the telephone, via a computer-assisted telephone interview (CATI). Businesses' contact details were obtained from the ABS Australian Business Register (ABR). The sample was stratified by industry sector and business size. That is, businesses were selected from small (0–19 employees), medium (20–199 employees) and large (more than 200 employees) businesses, and from all 19 industries as defined in the Australian and New Zealand Standard Industrial Classification (ANZSIC) (see ABS & Statistics New Zealand 2006). The ANZSIC industry sector classifications used in the survey were:

- agriculture, forestry and fishing
- mining
- manufacturing
- electricity, gas, water and waste services
- construction
- wholesale trade
- retail trade
- accommodation and food services
- transport, postal and warehousing
- information media and telecommunications

- financial and insurance services
- rental, hiring and real estate services
- professional, scientific and technical services
- administrative and support services
- public administration and safety
- education and training
- health care and social assistance
- arts and recreational services
- other services.

The survey excluded government organisations, primarily due to the perceived sensitivities involved in asking government organisations to divulge information about computer security incidents.

The businesses included in the original sampling frame were stratified equally across industry sectors, resulting in an over-sampling of medium and large businesses and a corresponding under-sampling of small businesses compared with their proportion in the Australian business population (see Appendix 1).

In order to better represent businesses across Australia, data from the ABACUS survey were weighted by industry sector and business size (i.e. small, medium or large). Weighted data have been used throughout this report in order to estimate frequencies for all businesses across Australia. The process of weighting data involves

applying a formula to data provided by each respondent to make each response proportionate in relation to the broader population being sampled.

Table 3 shows the breakdown of respondents by industry sector and business size. Both the

unweighted and weighted numbers are provided to show where the sample under or overestimated the business population. Most respondents in the sample were from small businesses (n=3,290), followed by medium businesses (n=576) and then

Table 3 Respondents by industry sector and business size (percent)

	Small				Medium				Large			
	Unweighted		Weighted		Unweighted		Weighted		Unweighted		Weighted	
	n	%	n	%	n	%	n	%	n	%	n	%
Agriculture, forestry and fishing	334	10	280	8	23	4	23	6	2	1	1	4
Mining	156	5	12	<1	38	7	2	1	13	10	1	2
Manufacturing	192	6	197	5	58	10	45	12	15	11	3	12
Electricity, gas, water and waste services	114	3	10	<1	21	4	1	<1	5	4	<1	1
Construction	193	6	542	15	30	5	31	8	5	4	2	6
Wholesale trade	142	4	165	5	21	4	25	7	4	3	2	6
Retail trade	309	9	332	9	43	7	45	12	4	3	2	8
Accommodation and food services	116	4	198	6	30	5	55	14	9	7	3	9
Transport, postal and warehousing	174	5	177	5	24	4	14	4	7	5	1	4
Information media and telecommunications	128	4	30	1	17	3	4	1	8	6	1	2
Financial and insurance services	202	6	305	9	13	2	9	2	6	4	2	5
Rental, hiring and real estate services	130	4	138	4	17	3	13	3	3	2	1	2
Professional, scientific and technical services	233	7	474	13	19	3	29	7	7	5	2	7
Administrative and support services	116	4	143	4	19	3	23	6	5	4	4	15
Public administration and safety	56	2	14	<1	28	5	3	1	5	4	<1	1
Education and training	152	5	50	1	74	13	13	3	14	10	1	4
Health care and social assistance	248	8	211	6	40	7	25	6	12	9	3	9
Arts and recreational services	176	5	49	1	49	9	9	2	9	7	1	2
Other services	118	4	258	7	12	2	16	4	1	1	1	3
Don't know	1	<1	2	<1	0	0	0	0	0	0	0	0
Total	3,290	100	3,586	100	576	100	385	100	134	100	29	100

Note: due to rounding, percentages in this report may not sum to 100

Source: AIC, ABACUS 2008 [computer file, weighted and unweighted data]

large businesses (n=134). These data have been weighted (to 3,586 small, 385 medium and 29 large businesses) to accurately reflect the distribution of small, medium and large businesses across Australia. The differences between the unweighted and weighted numbers reflect the under-sampling of small businesses and slight over-sampling of medium and large businesses. Industry sectors were also weighted to reflect the distribution of these sectors across Australia's business population. Industry sectors that were over-sampled have been 'weighted down' and under-sampled ones 'weighted up' to accurately reflect this. For example, Table 3 shows that 156 small businesses from the mining sector responded to the ABACUS survey. As this is a substantial over-sampling of mining sector businesses, small businesses from the mining industry have been weighted down to 12. Conversely, only 193 small businesses from the construction sector responded to the ABACUS survey. As this is an under-sampling, small businesses from the construction sector have been weighted up to 542, to reflect their distribution in the Australian business population.

Weighting the data by business size and industry sector enables more reliable conclusions to be drawn about the in-scope business population. Appendix 1 contains a more detailed discussion of the methodology used for this research, including a detailed description of the weighting process.

In total, 4,000 usable ABACUS questionnaires were completed on paper, online or via CATI. Of in-scope businesses in the sampling frame, the overall response rate for the survey was 29 percent. Missing data have been excluded from analyses in this report. As such, totals do not always sum to 4,000.

Respondents were asked to identify the state or territory in which the majority of their business's staff were employed during the 12-month period ending 30 June 2007. Table 4 shows the distribution of business respondents among Australia's states and territories.

Participants were asked to indicate whether their business is considered to be a part of the critical infrastructure sector according to the TISN. The TISN defines critical infrastructure as *those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would detrimentally impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security* (see www.tisn.gov.au). Four percent of respondents who answered this question in the ABACUS survey indicated that their business belonged to the critical infrastructure. Of these, six percent indicated that their business belonged to the critical infrastructure. Thirty-four percent did not know whether their business belonged to the critical infrastructure.

Table 4 Respondents by state or territory of operation and business size (percent)

	Small				Medium				Large			
	Unweighted		Weighted		Unweighted		Weighted		Unweighted		Weighted	
	n	%	n	%	n	%	n	%	n	%	n	%
NSW	1,060	32	1,182	33	176	31	121	31	45	34	10	35
Vic	840	26	943	26	158	27	105	27	33	25	9	30
Qld	611	19	673	19	114	20	80	21	23	17	5	17
WA	352	11	354	10	58	10	33	9	18	13	3	11
SA	260	8	271	8	46	8	31	8	10	7	1	4
Tas	85	3	81	2	15	3	11	3	3	2	<1	3
NT	33	1	28	1	2	<1	<1	<1	1	1	<1	<1
ACT	49	1	55	2	7	1	4	1	1	1	<1	<1
Total	3,290	100	3,586	100	576	100	385	100	134	100	29	100

Source: AIC, ABACUS 2008 [computer file, weighted and unweighted data]

The survey also asked respondents to estimate the turnover of their business during the 12-month period ending on 30 June 2007. As might be expected, small businesses were more heavily concentrated in the lower annual turnover categories, particularly those under \$10m, while medium and large businesses were more heavily concentrated in the higher categories, particularly those between \$1m–9,999,999 and \$10m–99,999,999. Table 5 shows the distribution of annual turnover of small, medium and large business respondents.

Table 5 Annual turnover of respondents by business size (percent) (\$)				
	Small	Medium	Large	Weighted n
Less than 99,999	21	1	0	686
100,000–499,999	40	4	1	1,273
500,000–999,999	15	6	5	505
1m–9,999,999	20	59	14	855
10m–99,999,999	1	26	74	142
1b	0	0	1	<1
Don't know	2	5	5	90
Total	100	100	100	3,551

Note: excludes 449 missing answers (411 from small, 35 from medium, 3 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Respondents’ roles within businesses

Respondents held a variety of roles within their respective businesses. Small and medium business respondents were most likely to identify themselves as the owner, director, Chief Executive Officer or Managing Director of their business, followed by general management or operations management positions. Large business respondents were most likely to identify as holding the Chief Information Officer or another information technology management role, followed by Chief Financial Officer or similar financial management role and general management or operations management positions. Table 6 shows the breakdown of respondents’ roles within their businesses.

Table 6 Respondents’ roles within businesses, by business size (percent)				
	Small	Medium	Large	Weighted n
Owner/director/CEO/MD	75	33	7	2,780
General management/operations management	11	25	13	499
CFO/financial management	6	17	13	267
CIO/IT management	2	19	62	145
Fraud/security control	<1	0	1	2
Administration/office/clerical	3	3	1	116
Accounts/bookkeeping/payroll	1	1	1	47
Other	3	3	2	102
Total	100	100	100	3,958

Note: Excludes 42 missing answers (37 from small, 5 from medium, fewer than 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Respondents’ knowledge of and ability to use information technology

Respondents were asked to rate their level of knowledge about, and ability to use, information technology. The highest proportions of small (53%) and medium (41%) business respondents rated their *knowledge* of information technology as ‘moderate’, whereas the highest proportion of large businesses (38%) rated their knowledge of information technology as ‘high’. Small business respondents were most likely to rate their *ability* to use information technology as ‘moderate’ (52%). Medium (42%) and large (39%) business respondents were most likely to rate their ability as ‘high’ (see Table 7).

Table 7 Respondents' level of knowledge of and ability to use information technology, by business size (percent)

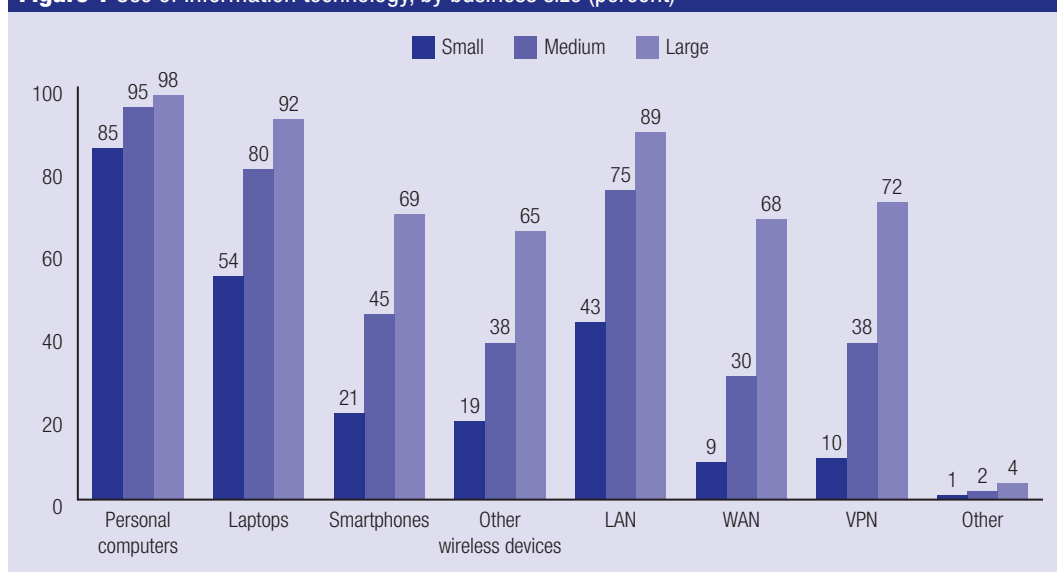
	Level of knowledge				Ability to use			
	Small	Medium	Large	Weighted n	Small	Medium	Large	Weighted n
Very low	6	2	1	214	5	1	1	183
Low	14	6	0	515	12	7	0	439
Moderate	53	41	26	2,025	52	33	24	1,893
High	21	37	38	889	24	42	39	992
Very high	6	15	35	268	6	16	36	280
Total	100	100	100	3,910 ^a	100	100	100	3,787 ^b

a: Excludes 90 missing answers (76 from small, 13 from medium, fewer than 1 from large businesses)

b: Excludes 213 missing answers (188 from small, 22 from medium, 3 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Figure 1 Use of information technology, by business size (percent)



Note: n=3,976. Excludes 24 missing answers (19 from small, 5 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Businesses' use of information technology

Ninety-two percent of respondents overall (92% of small and 99% of medium and large businesses) reported that their business used some form of information technology within the 12-month period. Businesses were asked about their use of:

- *personal computers*: desktop computers—other than laptops—designed for the use of business applications such as word processing or account keeping
- *laptops*: portable computers that are able to perform the same functions as a personal computer
- *smart phones*: mobiles with personal computer-like functionality such as the ability to send and receive emails and access the internet
- *other wireless devices*: devices that operate, or the components of which operate, without the use of wires
- *local area networks*: computer networks that encompass a limited area such as a building or office

- *wide area networks*: computer networks that encompass a large geographical area, such as a group of buildings or separate offices that are located in separate states or countries
- *virtual private networks*: networks that are established via the use of public wires, such as telephone or broadband internet wires.

Of those businesses that used some type of information technology, 86 percent reported using personal computers, 57 percent laptops, 24 percent smart phones, 21 percent other wireless devices, 46 percent a local area network, 12 percent a wide area network and 13 percent a virtual private network. One percent reported the use of ‘other’ information technologies (see Figure 1). Figure 1 shows the proportion of small, medium and large businesses that reported using each type of information technology.

A consistent pattern emerged in relation to types of information technology used by businesses of varying sizes. The ABACUS data clearly show that a greater proportion of large businesses reported using each type of information technology than medium businesses and that, in turn, a greater proportion of medium businesses reported using each type of information technology than small businesses.

Expenditure on information technology

The ABACUS survey asked participants whose businesses used information technology to estimate their business’s total information technology

expenditure for the 12-month period ending 30 June 2007. Information technology expenditure was defined in the ABACUS survey as *all types of expenditure relating to your business’s information technology. These may include the cost of information technology training, software and hardware and salaries for information technology staff*. As might be expected, small businesses tended to report lower overall information technology expenditure than medium businesses and medium businesses in turn reported lower information technology expenditure than large businesses. Table 8 shows the breakdown of total information technology expenditure across small, medium and large businesses.

Table 8 Total information technology expenditure, by business size (percent) (\$)				
	Small	Medium	Large	Weighted n
Less than 1,000	27	5	2	814
1,000–9,999	52	27	10	1,630
10,000–24,999	12	23	6	446
25,000–74,999	3	17	8	136
75,000–99,999	<1	3	<1	20
100,000 or more	1	16	64	106
Don't know	5	9	11	178
Total	100	100	100	3,330

Note: Excludes 307 businesses with no information technology and 364 missing answers (328 from small, 33 from medium, 3 from large businesses)
Source: AIC, ABACUS 2008 [computer file, weighted data]



Preventing computer security incidents against Australian businesses

The ABACUS questionnaire asked businesses a number of questions about the measures they undertook to prevent computer security incidents during the 12 months ending on 30 June 2007. Respondents were asked to identify the computer security tools and policies their business had in place during this time, as well as the amount and type of their business's expenditure on computer security. Businesses were also asked about the outsourcing of computer security functions, and how outsourced and other computer security functions were evaluated. Additionally, the ABACUS survey asked respondents to identify the types of computer security awareness-raising initiatives they were familiar with.

The measures businesses in the ABACUS study took to prevent computer security incidents will be presented in this section. Where appropriate, the findings of previous surveys will be compared with the ABACUS findings.

Businesses' use of computer security tools

Respondents were asked about their business's use of a number of broad categories of computer security tools. These included:

- *physical security tools*: using devices such as locks to secure computer hardware
- *cryptographic and authentication tools*: cryptography is a means of scrambling ordinary text into 'ciphertext', then back again. This enables securing of private information sent through public networks by making it unreadable to anyone except the person/s holding the mathematical key or knowledge to decrypt the information. Authentication software or hardware is designed to verify the identity of a user, process or device, often as a prerequisite to allowing access to resources in a system
- *anti-fraud and malware tools*: software or hardware designed to prevent fraud or malware, such as viruses
- *detection and monitoring tools*: software or hardware designed to monitor the use of a specific computer system or network
- *security management tools*: software or hardware designed to manage and improve the security of computer systems and networks.

Eighty-five percent of businesses that used information technology of any kind during the period reported using some type of computer security tool. A far greater proportion of small businesses (15%) than medium (6%) or large (4%) businesses with information technology reported using no computer security tools.

A clear pattern can be observed in the use of computer security tools across small, medium and large businesses. A greater proportion of large businesses than medium businesses reported using each of the types of computer security tool listed in the ABACUS survey. In turn, a greater proportion of medium businesses than small businesses reported using each security tool. The only exception is the ‘other tools’ category, as indicated in Table 9.

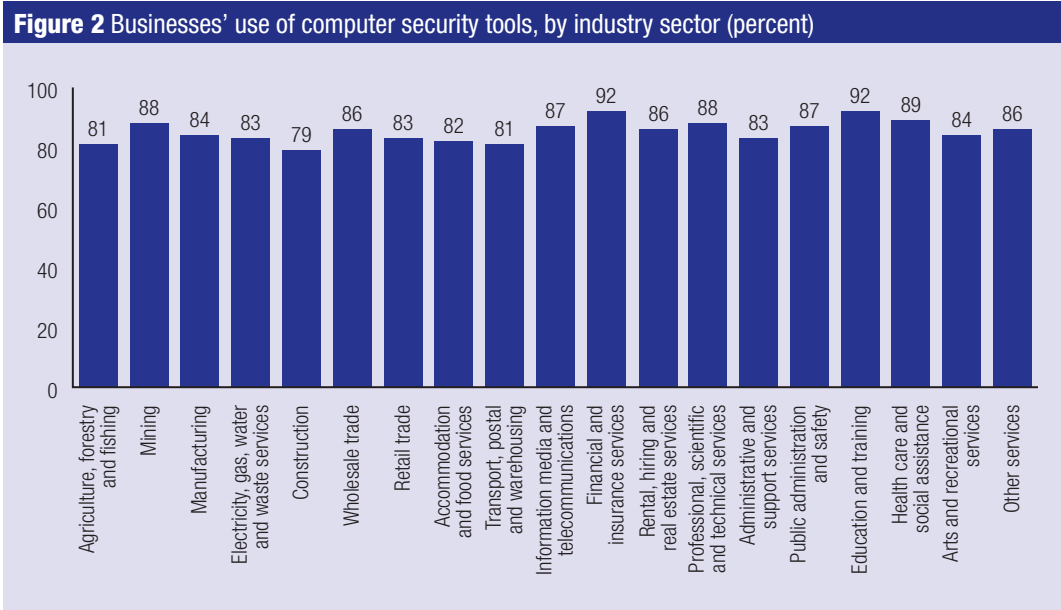
Table 9 Use of computer security tools, by business size (percent)				
	Small	Medium	Large	Weighted n
Physical security	49	78	90	1,900
Cryptographic and authentication tools	58	83	91	2,222
Anti-fraud and malware tools	87	94	95	3,207
Detection and monitoring tools	38	61	76	1,502
Security management tools	73	87	91	2,727
Other tools	1	<1	5	19

Note: n=3,658. Excludes 307 businesses with no information technology and 36 missing answers (34 from small, 2 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Over three-quarters of businesses that reported using some type of information technology from each industry sector reported using one or more computer security tools. As Figure 2 shows, the proportion of businesses using one or more computer security tools ranged from 79 percent of construction industry businesses to 92 percent of businesses from the financial and insurance services and education and training sectors. Figure 2 shows the proportions of businesses from each industry sector that reported using one or more computer security tools during the 2006–07 financial year.

The ABACUS data indicate that far fewer businesses report using most computer security tools than previous surveys on computer security incidents against businesses have found. In the sections that follow, findings from the ABACUS survey about particular computer security tools (such as anti-virus software) are presented alongside those of previous surveys. Possible explanations for the differences among surveys are offered later in this section of the report, in a general discussion of key findings about businesses’ use of computer security tools.



Note: n= 3,657. Excludes 307 businesses with no information technology and 36 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

Physical computer security tools

Business respondents that used information technology were asked to identify the types of physical security their business used during the financial year ending 30 June 2007. As previously stated, physical security tools were defined as *using devices, such as locks, to secure computer hardware*. Respondents were asked about *keeping servers in secure rooms, limiting access to workstations, physically securing laptop computers, and physically securing wireless devices*. These tools were deemed self-explanatory and were not individually defined.

Fifty-two percent of respondents (49% of small, 78% of medium, 90% of large businesses) reported using physical security tools. As Figure 3 indicates, the highest proportion of medium (59%) and large businesses (76%) reported keeping servers in secure rooms. The highest proportion of small businesses (28%) reported limiting access to work stations.

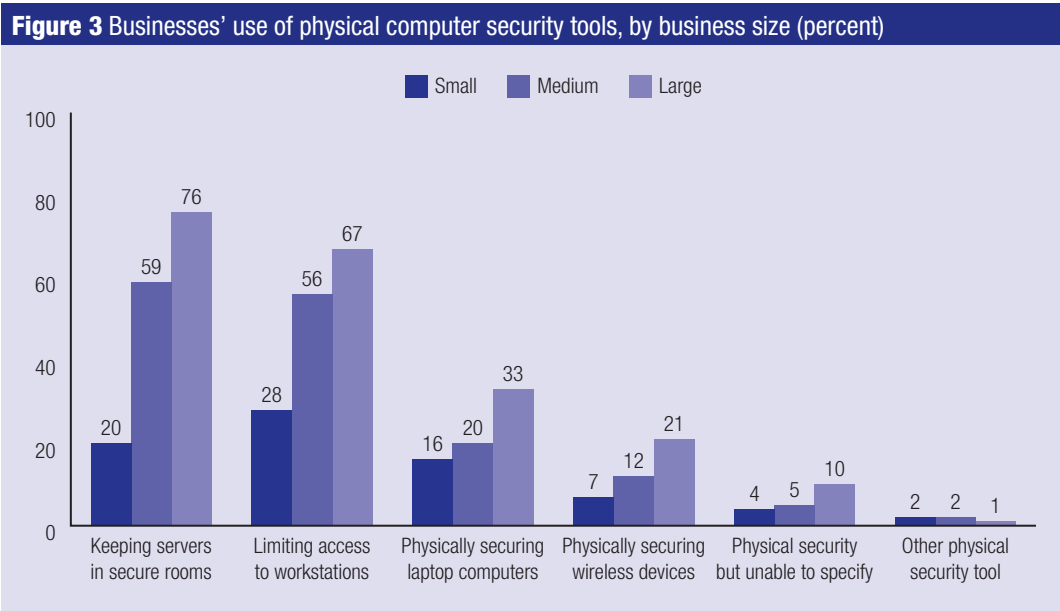
Questions about physical security measures are not common in surveys on computer security incidents against businesses. Of the previous surveys on this topic, only the ABS (2007: 12) *Business use of information technology* survey asked respondents

to indicate whether they had used any physical security tools in securing their business's information technology security. Thirty-one percent of respondents to the ABS survey indicated that they had used physical security tools.

Physical security tools were the only computer security tools that a considerably higher proportion of ABACUS respondents reported using in comparison with respondents to a previous survey. This may be due to the fact that the ABACUS survey described a number of physical security measures, such as 'keeping servers in secure rooms' and 'physically securing laptop computers'. The ABS survey appears to have simply asked respondents whether they used 'physical security' without further detailing what this category may include. This may help explain the higher proportion of ABACUS respondents that reported using physical security tools.

Cryptographic and authentication tools

Businesses that used information technology were asked to identify the types of cryptographic and authentication tools their business used during the



Note: n=3,658. Excludes 307 businesses with no information technology and 36 missing answers (34 from small, 2 from medium businesses)
Source: AIC, ABACUS 2008 [computer file, weighted data]

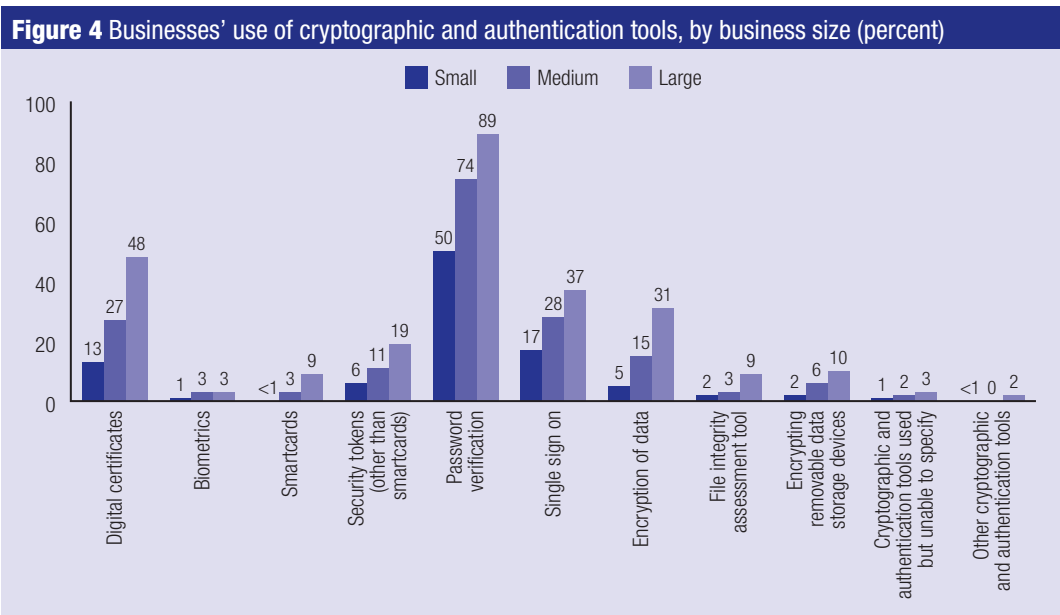
financial year ending 30 June 2007 (Figure 4).
Businesses were asked about:

- *digital certificates*: electronic documents signed by a trusted Certification Authority that identifies the key holder and the affiliated business entity, binds the key holder to a public/private key pair and contains other information required by the certificate profile
- *biometrics*: use of a person's physical or behavioural characteristics, such as retinal scans, as a form of identification and authentication
- *smartcards*: plastic cards containing integrated circuits for information system access and identification and the holding of digital credentials and electronic value tokens
- *security tokens other than smartcards*: hardware devices designed to provide two-factor authentication by generating a one-time authentication key, in addition to a password or pin, that allows access to a network or system resources
- *password verification*: the use of a password that is linked to an individual user account that allows access to network or system resources

- *single sign on*: an identity management mechanism that allows account holders to authenticate themselves once when accessing interconnected network and system resources
- *encryption of data*: the process of scrambling or encoding of information to ensure that only the intended recipient can read the information
- *file integrity assessment tools*: software or hardware used to verify the integrity of the contents of files
- *encrypting removable data storage devices*: process of scrambling or encoding information on removable storage devices to ensure that only the intended recipient can read the information.

Sixty-one percent of businesses (58% of small, 83% of medium, 91% of large businesses) with information technology reported using cryptographic and authentication tools. Figure 4 shows the proportions of small, medium and large businesses that reported using each cryptographic and authentication tool.

Fifteen percent of ABACUS respondents (13% of small, 27% of medium, 48% of large businesses) reported using digital certificates. Both AusCERT's



Note: n=3,658. Excludes 307 businesses with no information technology and 36 missing answers (34 from small, 2 from medium businesses)
Source: AIC, ABACUS 2008 [computer file, weighted data]

(2006) most recent survey and New Zealand's survey (Quinn 2006: 14) found higher proportions of businesses (47% and 17% respectively) reporting using this type of computer security tool.

Only one percent of ABACUS respondents (1% of small, 3% of medium, 3% of large businesses) with information technology used biometric tools. One percent of respondents to Quinn's New Zealand survey also reported using biometrics. This compares with five percent of respondents to the AusCERT survey, 18 percent of Richardson's US (2007: 18) respondents and 20 percent of global respondents to Deloitte Touche Tohmatsu's (2007: 29) survey.

One percent of ABACUS respondents (<1% of small, 3% of medium, 9% of large businesses) used smartcards. Greater proportions of respondents to the New Zealand (24%), AusCERT (24%) and Deloitte Touche Tohmatsu (26%) surveys reported using smartcards, as did respondents to Richardson's survey in the United States (35%).

Seven percent of ABACUS respondents (6% of small, 11% of medium, 19% of large businesses) with information technology used security tokens other than smartcards. Deloitte Touche Tohmatsu found that a far greater proportion of their respondents (51%) reported using security tokens. It is important to note here that in the AusCERT, New Zealand and Richardson surveys, the categories of smartcards and other security tokens may overlap (see above).

Fifty-two percent of ABACUS respondents (50% of small, 74% of medium, 89% of large businesses) used password verification tools. Proportions of businesses using password-related technologies vary considerably among surveys on computer security incidents against businesses. A surprisingly low proportion of respondents to Quinn's survey of businesses in New Zealand (28%) reported using reusable passwords. Eighty-four percent of the Computer Emergency Response Team et al. respondents used 'account/password management policies' and 51 percent of Richardson's respondents used 'static account login/password' technologies. It is unclear why there is such a discrepancy among these surveys, although differences in definitions of password tools are likely to be an important factor.

Eighteen percent of businesses that used information technology of some kind (17% of small, 28% of medium, 37% of large businesses) reported using single sign-on tools. Twenty-four percent of respondents to Quinn's survey of New Zealand businesses used this type of computer security tool.

Seven percent of respondents (5% of small, 15% of medium, 31% of large businesses) reported using encryption of data to maintain computer security. Sixty-six percent of Deloitte Touche Tohmatsu's respondents used encryption of some kind. Sixty-six percent of Richardson's respondents used encryption for data in transit and 47 percent used encryption for data in storage. Forty-six percent of AusCERT's respondents used encrypted login/sessions, and 39 percent of respondents in New Zealand used encrypted login.

Three percent of ABACUS respondents with information technology (2% of small, 3% of medium, 9% of large businesses) used file integrity assessment tools. Seventeen percent of respondents to AusCERT's survey reported using this type of computer security tool.

Three percent of ABACUS respondents (2% of small, 6% of medium, 10% of large businesses) reported encrypting removable data storage devices. A far higher proportion (47%) of respondents to Richardson's survey in the United States reported using this computer security tool. This category may overlap with the encryption of data category in some surveys (see above).

Anti-fraud and malware computer security tools

Businesses that used information technology were asked to identify which anti-fraud and malware tools their business used during the 12-month period. The ABACUS survey asked respondents about their use of:

- *anti-spam filters*: software/hardware used to identify and block unsolicited email used to commit fraud
- *anti-virus software*: software tools designed to identify, thwart and eliminate malicious code such as viruses

- *anti-spyware software*: software designed to detect and remove spyware from a system
- *anti-phishing software*: software designed to detect and prevent phishing attacks and resultant fraud.

Eighty-eight percent of businesses with information technology reported using some type of anti-fraud and malware tool (87% of small, 94% of medium, 95% of large businesses). Figure 5 shows the proportions of small, medium and large businesses that reported using each computer security tool within this category.

Sixty-four percent of business respondents who used information technology (63% of small, 77% of medium, 85% of large businesses) reported using anti-spam filters. This is a slightly larger proportion than that found by the ABS (62%), but smaller than that found by Deloitte Touche Tohmatsu (86%) and AusCERT (90%).

Eighty-five percent of respondents (84% of small and 91% of medium and large businesses) reported using anti-virus software. Other surveys that measured use of anti-virus software found higher proportions of respondents who used this than did ABACUS. Richardson, AusCERT and the Department of Trade and Industry all found that

98 percent of respondents used anti-virus software, and Quinn and Deloitte Touche Tohmatsu found that 99 percent of respondents did so.

Fifty-nine percent of respondents (58% of small, 64% of medium, 74% of large businesses) reported using anti-spyware software. This is a slightly higher proportion than that found by Deloitte Touche Tohmatsu (58%), but lower than that found by the Department of Trade and Industry (74%) and Richardson (80%).

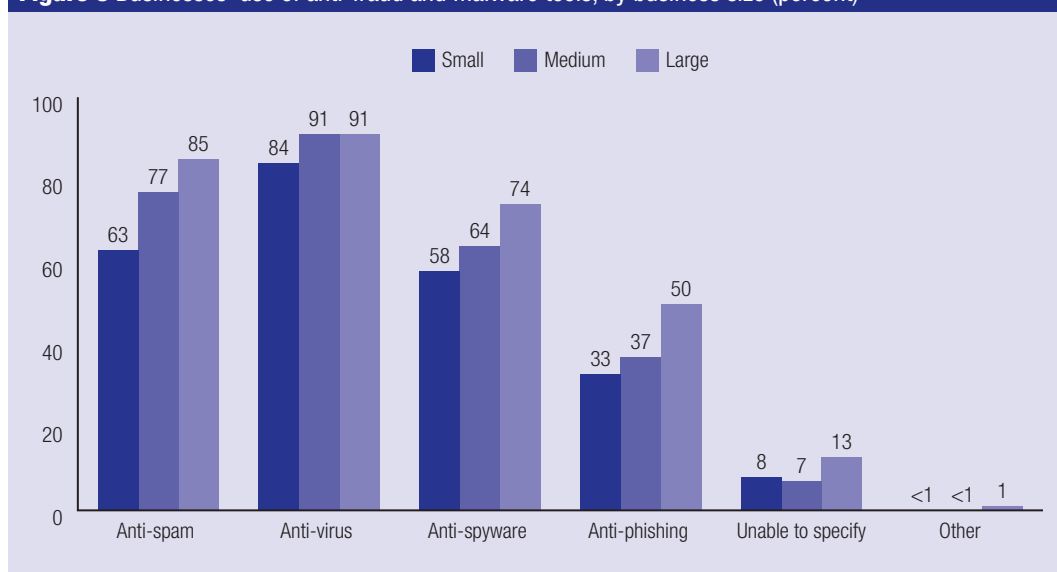
Thirty-four percent of business respondents that used information technology (33% of small, 37% of medium, 50% of large businesses) reported using anti-phishing software.

Previous surveys on computer security incidents against businesses have not collected data on anti-phishing software.

Detection and monitoring computer security tools

Business respondents that reported some type of information technology were asked to identify which detection and monitoring tools their business used.

Figure 5 Businesses' use of anti-fraud and malware tools, by business size (percent)



Note: n= 3,658. Excludes 307 businesses with no information technology and 36 missing answers (34 from small, 2 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

The ABACUS survey asked respondents about their use of:

- *internet content filtering/image filtering or monitoring*: software or hardware designed for monitoring and limiting access to inappropriate information or data configured according to a business's security policy
- *intrusion detection systems*: software applications designed to protect services by detecting inappropriate, incorrect or anomalous activities that cannot usually be detected by a conventional firewall
- *intrusion prevention systems*: software or hardware designed to protect computers from exploitation by identifying and blocking potentially malicious activity in real-time.

Forty-one percent of respondents reported using detection and monitoring tools (38% of small, 61% of medium, 76% of large businesses). Figure 6 shows the proportions of small, medium and large businesses that reported using each computer security tool within this category.

Twenty-five percent of businesses that used some kind of information technology (23% of small, 42% of medium, 69% of large businesses) reported using internet content/image filtering/monitoring. This is a

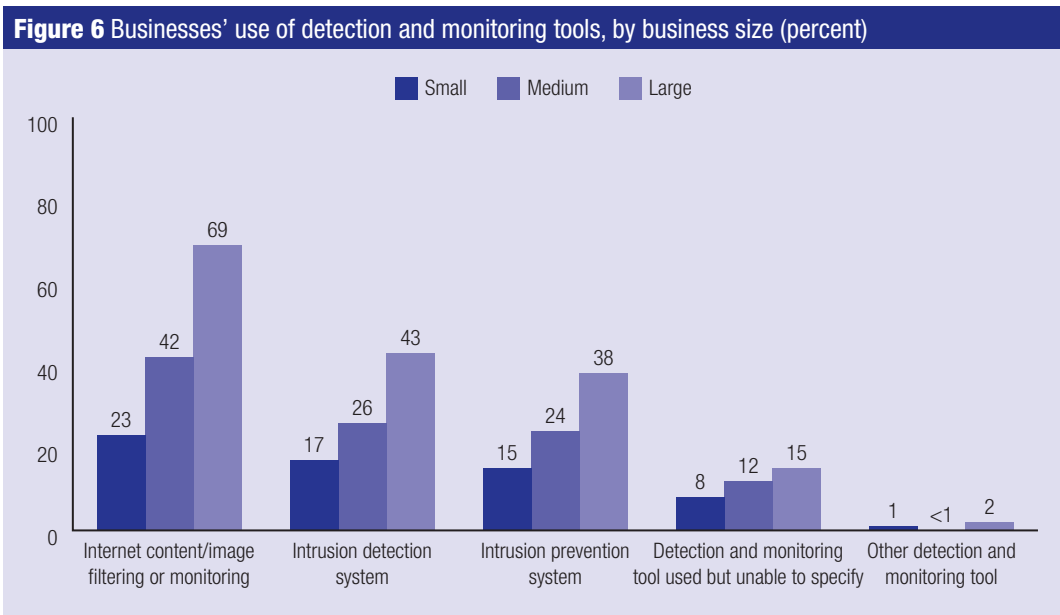
much lower proportion than was found in Quinn's and Deloitte Touche Tohmatsu's surveys (78% each).

Eighteen percent of ABACUS respondents (17% of small, 26% of medium, 43% of large businesses) reported using an intrusion detection system. This is a lower proportion than was found in AusCERT's (44%), Quinn's (58%) and Deloitte Touche Tohmatsu's (76%) surveys.

Sixteen percent of respondents (15% of small, 24% of medium, 38% of large businesses) used an intrusion prevention system. Higher proportions of respondents reported using this type of computer security tool in both Richardson's (47%) and Deloitte Touche Tohmatsu's (55%) surveys. Importantly, respondents to surveys on computer security tools may inadvertently conflate *intrusion detection* and *intrusion prevention* tools, and it is important to be mindful of this when interpreting these results.

Security management computer security tools

Finally, businesses that used information technology were asked to identify which security management tools their business had used. The ABACUS survey asked respondents about their use of:



Note: n= 3,658. Excludes 307 businesses with no information technology and 36 missing answers (34 from small, 2 from medium businesses)

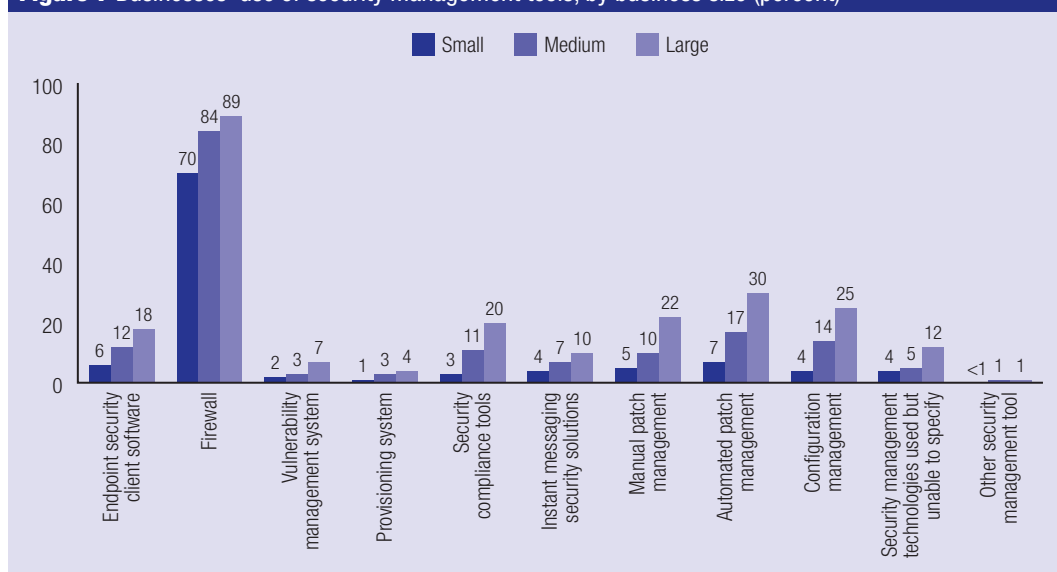
Source: AIC, ABACUS 2008 [computer file, weighted data]

- *endpoint security software*: a suite of software and hardware, designed to work to prevent security breaches and to conform to defined enterprise and desktop security policies at endpoints. The latter can be an individual computing or storage device such as a client workstation for a network or personal computing device including laptops, desktop computers and Personal Digital Assistants
- *firewalls*: software or hardware designed for the protection of a network from unauthorised access that permits, denies or provides proxy data connections configured according to an organisation's security policy
- *vulnerability management systems*: a process in which vulnerabilities are found and fixed and vulnerable systems are shielded. This includes configuration policy compliance, threat information, asset clarification, prioritisation and workflow
- *provisioning systems*: systems that allow the management of user accounts and profiles that are linked to a person across an information technology environment through user roles and business rules
- *security compliance tools*: software applications that enforce corporate and/or regulatory policies and standards
- *instant messaging security solutions*: software applications that enforce instant messaging usage policies, such as the types of instant messaging applications that are allowed
- *manual patch management*: the process of controlling the deployment and maintenance of interim software releases, such as software updates, and security patches into production environments
- *automated patch management*: process of patch management with minimal human intervention, that enables automated analysis targeting and distribution of granular level patches and quality-assurance testing
- *configuration management*: the establishment of approved changes to the configuration of a computer system or network and the interrelation between system components.

Seventy-five percent of respondents reported using security management tools (73% of small, 87% of medium, 91% of large businesses). Figure 7 shows the proportions of small, medium and large businesses that reported using each computer security tool within this category.

Seven percent of businesses with information technology reported using endpoint security client software (6% of small, 12% of medium, 18% of large

Figure 7 Businesses' use of security management tools, by business size (percent)



Note: n=3,658. Excludes 307 businesses with no information technology and 36 missing answers (34 from small, 2 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

businesses). Richardson's survey of businesses in the United States—the only existing research study to survey respondents on this aspect of computer security—found that 27 percent of business respondents reported using this type of security tool.

A majority of ABACUS respondents (72%) reported using a firewall as part of their approach to information technology security (70% of small, 84% of medium, 89% of large businesses). This is a lower proportion than those found in other surveys on computer security incidents against businesses. The ABS found that a slightly higher proportion (73%) of respondents used this security tool. Quinn and Deloitte Touche Tohmatsu both found that 96 percent of respondents used firewalls, Richardson found that 97 percent of respondents did so, and AusCERT found that 98 percent of their respondents reported using this type of computer security tool.

Just three percent of ABACUS respondents reported using a vulnerability management system during the 12-month period ending 30 June 2007 (2% of small, 3% of medium, 7% of large businesses). This is a much lower proportion of businesses than was found by Deloitte Touche Tohmatsu (55%) and Richardson (63%).

A very small proportion of respondents to the ABACUS survey (1%) reported using a provisioning system as part of their information technology security strategy during the 12-month period ending 30 June 2007 (1% of small, 3% of medium, 4% of large businesses). Deloitte Touche Tohmatsu found a much higher proportion of respondents (35%) reported using provision systems.

Security compliance tools were used by four percent of ABACUS respondents whose businesses' used some type of information technology (3% of small, 11% of medium, 20% of large businesses). The only other study to survey respondents on this particular information technology tool was Deloitte Touche Tohmatsu, who found that a much higher proportion of respondents (39%) reported using this type of security tool.

Four percent of ABACUS respondents (4% of small, 7% of medium, 10% of large businesses) reported using instant messaging security solutions. Fourteen percent of Deloitte Touche Tohmatsu's respondents reported using this type of computer security tool.

A number of computer security tools that the ABACUS study surveyed respondents in regards to were not included in existing surveys on computer security incidents against businesses. The ABACUS study found that five percent of respondents (5% of small, 10% of medium, 22% of large businesses) used manual patch management and eight percent (7% of small, 17% of medium, 30% of large businesses) used auto-patch management. Five percent of respondents (4% of small, 14% of medium, 25% of large businesses) to the ABACUS survey used configuration management in the 12-month period ending 30 June 2007.

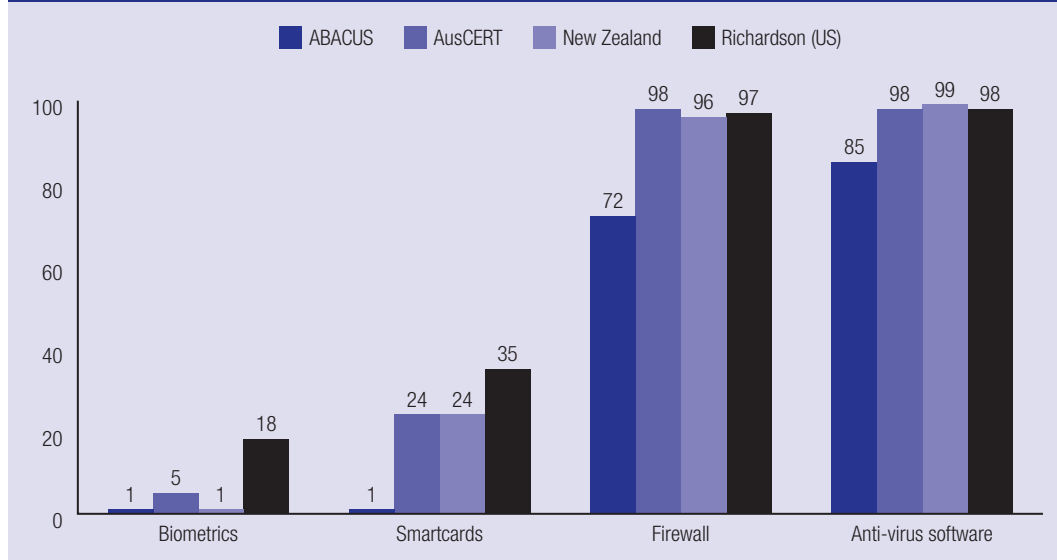
Key findings on businesses' use of computer security tools

Computer security tools belonging to the anti-fraud and malware tools category were the most widely used during the reporting period with anti-spam, anti-virus and anti-spyware software being used by a majority of small, medium and large businesses in Australia. The single most widely used computer security tool was anti-virus software, which 84 percent of small and 91 percent of medium and large businesses with information technology reported using. Security management tools was the category of computer security tools least likely to be used by businesses, with the notable exception of firewalls, which were used by 70 percent, 84 percent and 89 percent of small, medium and large businesses respectively.

A clear pattern is also evident from the data on the types of computer security tools within each of the above categories. For almost every computer security tool, a greater proportion of large businesses reported usage than medium businesses and a greater proportion of medium businesses reported usage than small businesses.

With very few exceptions, smaller (sometimes dramatically smaller) proportions of ABACUS respondents reported using each of the listed computer security tools than respondents to previous surveys in this field. Figure 8 shows the proportions of ABACUS respondents that reported

Figure 8 Computer security tools used by businesses, comparison with other surveys (percent)



Note: ABACUS n=3,658. Excludes 307 businesses with no information technology and 36 missing answers (34 from small, 2 from medium businesses). AusCERT n=389, New Zealand n=112 and Richardson n=484

Source: AIC, ABACUS 2008 [computer file, weighted data]

using selected computer security tools in comparison with the AusCERT, New Zealand and Richardson (US) surveys.

There are a number of possible explanations for this discrepancy in findings.

- The ABACUS survey sampled small, medium and large businesses and then weighted data to reflect the Australian business population. As outlined earlier in this report, many existing surveys on computer security incidents against businesses did not undertake a representative sample of businesses. A number excluded sole traders, sampled large businesses only, or boosted their sample of large businesses artificially. This could impact upon the overall proportion of respondents reporting using computer security tools. For example, small businesses are less likely to have tools in place but make up the majority of businesses in Australia.
- The ABACUS study also surveyed businesses from all industry sectors, whereas other surveys have focused on computer security organisations only. It is reasonable to assume that computer security organisations have high levels of use of computer security tools and this is very likely to have affected the difference in results among these surveys.

- Government organisations were also excluded from the ABACUS survey. As government organisations were included in a number of previous surveys on computer security incidents against businesses, this may have impacted findings. It may be the case that government organisations are more likely to make use of computer security tools than private sector businesses, particularly small businesses.
- Unlike a number of previous surveys, the ABACUS survey did not sample businesses based on their annual turnover. The ABACUS study has a larger proportion of respondents with low annual turnovers than other surveys, so it is therefore likely that many ABACUS respondents have smaller budgets for computer security tools.
- The ABACUS data may reveal low levels of e-literacy among business owners and this may have impacted on the finding of lower overall use of computer security tools. It is possible, for example, that businesses may have computer security tools such as anti-virus software or firewalls that were installed automatically on their computer. As such, these respondents may have computer security tools that they are not aware of.

- Finally, it is possible that particular computer security tools may simply be more popular in some cultural and/or geographical contexts. This may be the case in relation to controversial or very new technologies such as biometrics.

Businesses' use of computer security policies

Businesses that reported using one or more type of information technology were also asked about their use of a number of broad categories of computer security policies. These included:

- *staff related policies*: computer security policies that are directed at the staff of a business
- *security testing policies*: such as system audit policies or risk assessment policies
- *data related policies*: policies related to the handling, storage and security of data for a business
- *incident response policies*: policies that govern appropriate responses after a computer security incident has occurred
- *external business policies*: such as payment system supplier policies
- *wireless security policies*: policies that govern what types of security practices are used for and the protection of data that is stored and transferred between wireless devices.

Forty-two percent of businesses that used information technology of any kind reported using some type of computer security policy (38% of small, 72% of medium, 87% of large businesses). Importantly, 56 percent of businesses (60% of small, 27% of medium, 10% of large businesses) reported that they did not have any computer security policies in place. Less than half of small businesses—which comprise the majority of businesses in Australia—had active computer security policies in place during the reporting period.

A clear pattern can be observed in the use of computer security policies across small, medium and large businesses. A greater proportion of large businesses than medium businesses reported using each of the types of computer security policy listed

in the ABACUS survey. In turn, a greater proportion of medium businesses than small businesses reported using each security policy (see Table 10).

Table 10 Use of computer security policies, by business size (percent)

	Small	Medium	Large	Weighted n
Staff/user related policies	33	68	87	1,354
Security testing policies	10	25	48	441
Data related policies	31	63	85	1,268
Incident response policies	10	28	47	444
External business policies	8	21	27	339
Wireless security policies	15	36	56	626
Other policies	<1	<1	1	15

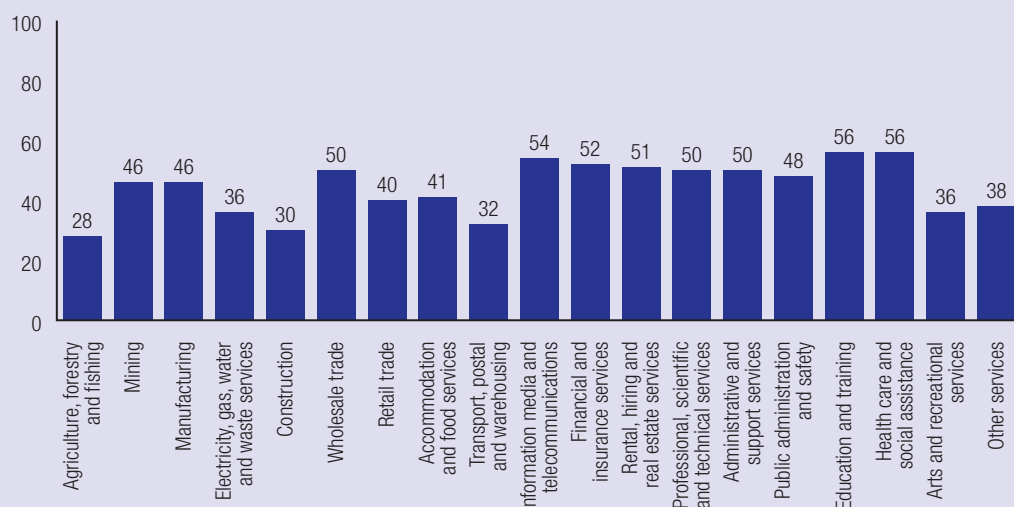
Note: n=3,616. Excludes 307 businesses with no information technology and 77 missing answers (76 from small, 1 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Businesses' use of computer security policies varied more across industry sectors than businesses' use of computer security tools. As Figure 9 shows, the proportion of businesses with one or more computer security policies in place ranged from 28 percent of agricultural, forestry and fishing sector businesses to 56 percent of education and training and health care and social assistance sector businesses. Figure 9 shows the proportions of businesses from each industry sector that reported having one or more computer security policy in place during the 12-month period ending 30 June 2007.

The ABACUS data indicate that far fewer businesses report using most computer security policies than previous surveys on computer security incidents against businesses have found. In the sections that follow, findings from the ABACUS survey about particular policies (such as acceptable use policies) are presented alongside those of previous surveys. Potential explanations for the differences among surveys are offered later in this section of the report, in a general discussion of key findings about businesses' use of computer security policies.

Figure 9 Businesses' use of computer security policies, by industry sector (percent)



Note: n=3,616. Excludes 307 businesses with no information technology, 77 missing answers and 66 'don't know' responses

Source: AIC, ABACUS 2008 [computer file, weighted data]

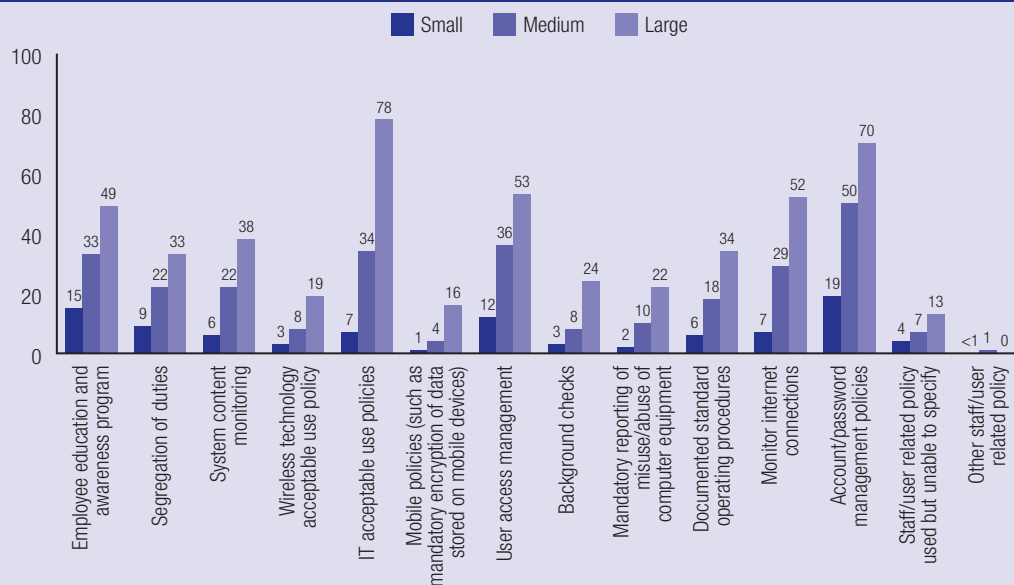
Staff/user-related computer security policies

Respondents were asked to identify which staff or user-related policies their business used. These included:

- *employee education and awareness programs*: courses and other activities to increase employees' awareness of computer security
- *segregation of duties*: segregation of duties occurs when no individual has control over two or more phases of a transaction or operation within a business environment. This is designed to prevent fraud
- *system content monitoring*: a system designed to specifically monitor information that is coming into and/or going out from a business's systems
- *wireless technology acceptable use policies*: policies that define what type of use is acceptable for a business's wireless technology, such as acceptable download limits for wireless devices
- *information technology acceptable use policies*: policies that define what type of use is acceptable for a business's information technology
- *mobile policies*: policies related to the use of mobile devices, such as what type of data may be stored on these devices
- *user access management policies*: policies that govern access rights of individuals on a business's systems
- *background checks*: policies that require verification of information provided by employees of a business, such as checking for a criminal history
- *mandatory reporting of misuse/abuse of computer equipment*: policies that require a person to report misuse or abuse of computer equipment as soon as they become aware of it
- *documented standard operating procedures*: a set of written instructions that governs the appropriate use of a business's information technologies
- *monitoring internet connections*: a policy that governs how individual users' internet activity is monitored
- *account/password management policies*: policies that specifically relate to users' account and password information, such as mandatory password length or frequency of password renewal.

Staff or user related policies were more likely to be used by businesses than any of the other categories of computer security policies. Overall, 37 percent of

Figure 10 Use of staff/user related computer security policies, by business size (percent)



Note: n=3,616. Excludes 307 businesses with no information technology and 77 missing answers (76 from small, 1 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

businesses that used some kind of information technology reported using a staff or user-related computer security policy. A higher proportion of large businesses (87%) than medium (68%) or small businesses (33%) reported using this type of policy. Figure 9 shows the proportions of small, medium and large businesses that reported using each staff/user related policy.

Seventeen percent of respondents with information technology (15% of small, 33% of medium, 49% of large businesses) used an employee education or awareness program. This was a considerably smaller proportion than that found by the research of the Computer Emergency Response Team et al. in the United States, which found that 43 percent of businesses had used new employee security training policies. It is important to note that respondents to the survey of the Computer Emergency Response Team et al. were asked whether their business had used computer security policies 'in an attempt to prevent or reduce security events'. It is possible that this approach may have resulted in a slightly lowered response rate, as businesses may adopt computer security policies for alternative reasons.

Segregation of duties was used by 10 percent of ABACUS respondents (9% of small, 22% of

medium, 33% of large businesses). This is a considerably lower proportion of respondents than Quinn and AusCERT found in their surveys (both 48%).

A much lower proportion of ABACUS respondents also reported using an information technology acceptable use policy than was found by existing surveys. Ten percent of businesses with information technology (7% of small, 34% of medium, 78% of large businesses) reported using this type of computer security policy. The research of the Computer Emergency Response Team et al. found that 80 percent of business respondents used an information technology acceptable use policy.

User access management policies were used by 15 percent of ABACUS respondents with information technology (12% of small, 36% of medium, 53% of large businesses). This is a much lower proportion of businesses using this type of policy than the AusCERT (93%) and New Zealand (96%) surveys found.

Background checks were used by just three percent of ABACUS respondents (3% of small, 8% of medium, 24% of large businesses) during the reporting period. This compares with 57 percent of respondents to the survey of the Computer

Emergency Response Team et al. that reported using background checks.

Seven percent of respondents to the ABACUS survey (6% of small, 18% of medium, 34% of large businesses) reported using documented standard operating procedures. Seventy-six percent of respondents to AusCERT’s most recent survey reported using this type of computer security policy.

Three percent of respondents reported using some kind of information technology policies involving the mandatory reporting of misuse or abuse of computer equipment (2% of small, 10% of medium, 22% of large businesses). Thirty-four percent of respondents to the survey by the Computer Emergency Response Team et al. reported using policies of this nature.

Nine percent of businesses (7% of small, 29% of medium and 52% of large businesses) reported using policies that monitored staff internet connections during the 12-month period ending 30 June 2007. This is a considerably lower proportion than was found in the survey by the Computer Emergency Response Team et al. (59%).

Account or password management policies were used by 22 percent of ABACUS respondents with information technology (19% of small, 50% of

medium, 70% of large businesses). The Computer Emergency Response Team et al. found that 84 percent of business respondents to their survey reported using this type of policy.

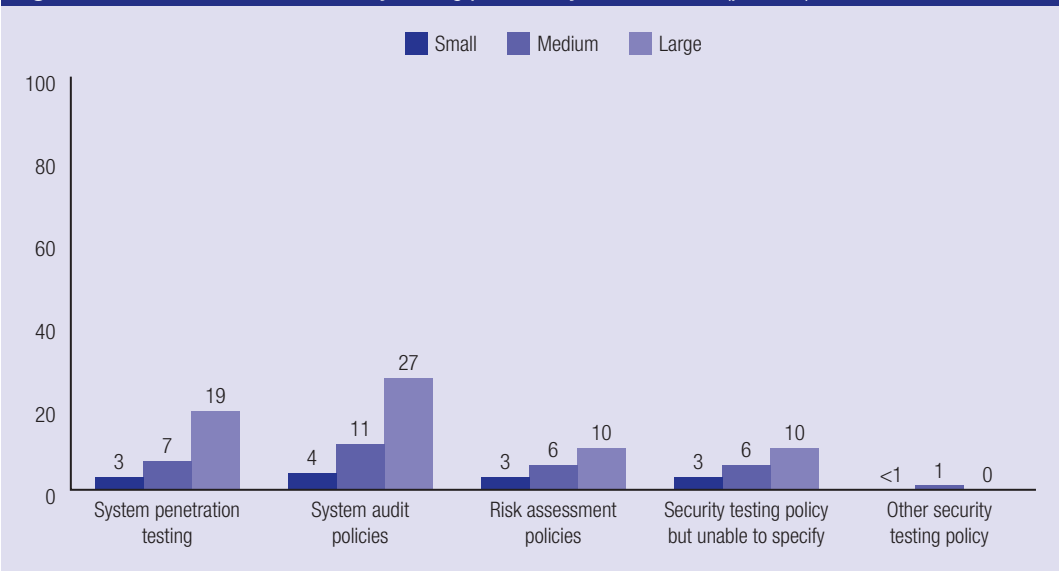
The ABACUS survey asked respondents to indicate whether their business had used a number of other staff/user related policies that have not previously been included in surveys on computer security incidents against businesses. The ABACUS data show that seven percent of businesses with information technology used system content monitoring, three percent used wireless technology acceptable use policies and two percent used mobile policies (such as mandatory encryption of data stored on mobile devices).

Security testing computer security policies

Businesses that used one or more types of information technology were asked about their use of various security testing policies. They were asked whether their business had used:

- *system penetration testing*: a method to evaluate the security of a computer, system or network by simulating an electronic attack

Figure 11 Businesses’ use of security testing policies, by business size (percent)



Note: n=3,616. Excludes 307 businesses with no information technology and 77 missing answers (76 from small, 1 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

- *system audit policies*: policies mandating audits of a business's computers, including issues such as the frequency and type of audits carried out and details of those responsible for undertaking those audits
- *risk assessment policies*: policies that govern the type and frequency of risk assessment of a business. Risk assessment is a process where the magnitude of potential loss and the probability it will occur are measured.

Security testing policies were used by 12 percent of respondents with information technology (10% of small, 25% of medium, 48% of large businesses). Figure 11 shows the proportions of business respondents that used each security testing policy.

System penetration testing policies were used by four percent of businesses. This figure varied across business size, with three percent of small businesses, seven percent of medium businesses and 19 percent of large businesses using policies of this nature. The Computer Emergency Response Team et al. found that 34 percent of respondents to their survey in the United States had used system penetration testing. Four percent of ABACUS respondents (3% of small, 11% of medium, 28% of large businesses) reported using system audit

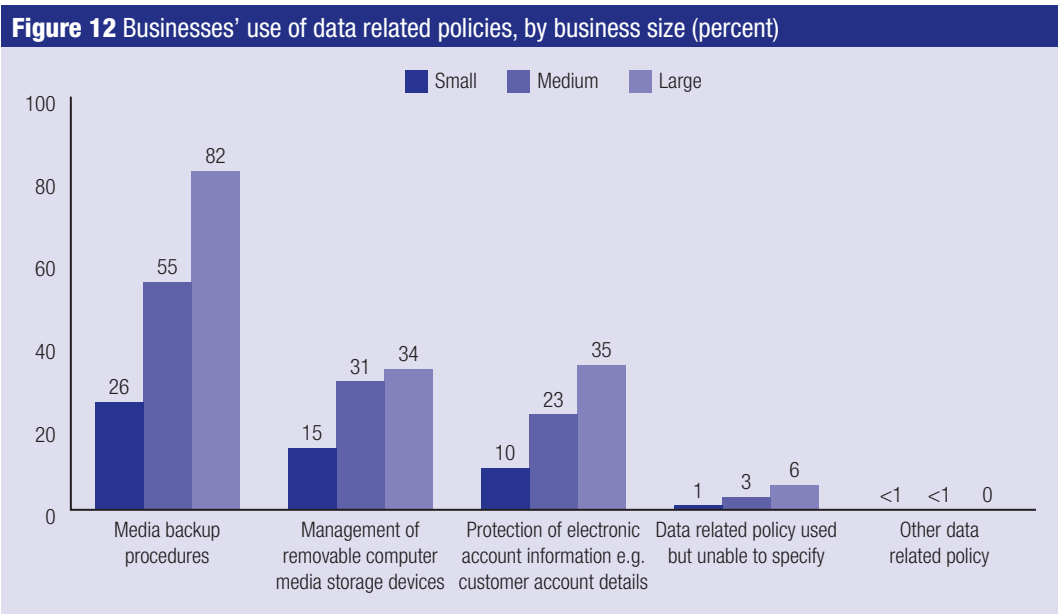
policies during the 12-month period ending 30 June 2007. This is a notably smaller proportion than found by the most recent AusCERT survey, which found that 58 percent of respondents had used this type of computer security policy.

Risk assessment policies were used by five percent of responding businesses (4% of small, 11% of medium, 27% of large businesses). The Computer Emergency Response Team et al. found that 42 percent of their respondents had used risk assessment policies.

Data related computer security policies

ABACUS respondents that reported that their business used information technology during the 12-month period ending on 30 June 2007 were also asked about their use of data related computer security policies. Businesses were asked whether they had used:

- *media backup procedures*: set policies and procedures that govern how the backup of data is recorded, stored and the frequency with which the backup occurs



Note: n=3,616. Excludes 307 businesses with no information technology and 77 missing answers (76 from small, 1 from medium businesses)
 Source: AIC, ABACUS 2008 [computer file, weighted data]

- *management of removable computer media storage devices*: policies that govern if, how and when removable computer media devices can be used
- *protection of electronic account information*: policies relating to the protection of customer, client or partner business information, such as credit card and personal details.

Thirty-five percent of all respondents reported utilising one or more data related computer security policies in the 12 months to 30 June 2007 (31% of small, 63% of medium, 85% of large businesses). Figure 12 shows the proportions of businesses that used each data related policy.

Media backup policies were used by 30 percent of ABACUS respondents (26% of small, 55% of medium, 82% of large businesses). This is a far lower proportion than has previously been found by AusCERT (95%) and Quinn (96%).

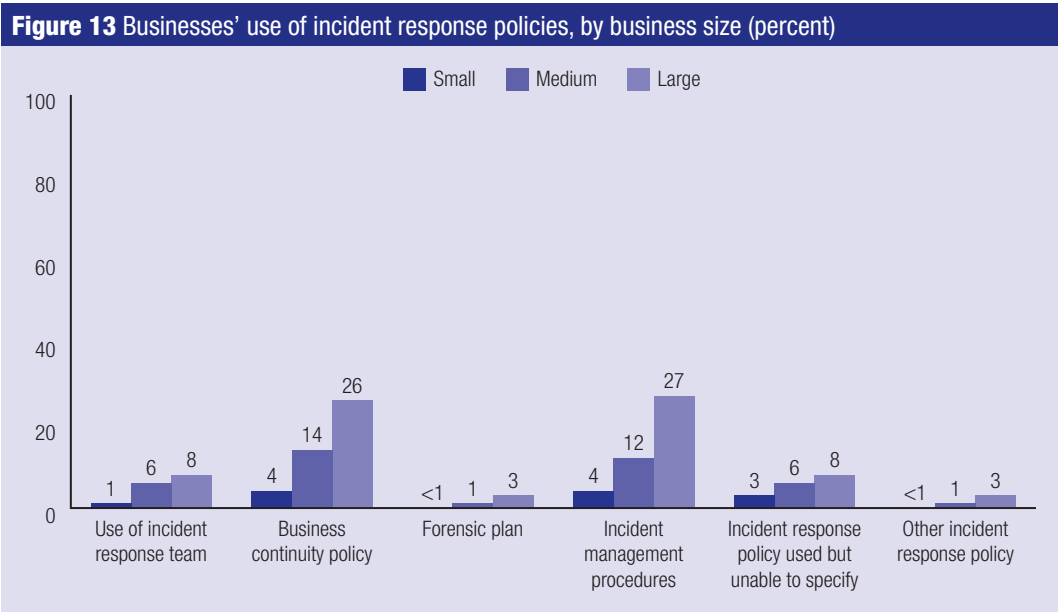
Seventeen percent of businesses with information technology reported using policies relating to the management of removable computer media storage devices (15% of small, 31% of medium, 34% of large businesses). Quinn’s research in New Zealand found that 42 percent of respondents had used this type of policy, and AusCERT found that 50 percent of respondents to their survey had done so.

Just 11 percent of ABACUS respondents reported having policies in place that aim to protect electronic account information such as customer account details (10% of small, 23% of medium, 35% of large businesses). This compares with 36 percent of respondents to the survey by the Computer Emergency Response Team et al. that reported having policies relating to the storage and review of email or computer files.

Incident response computer security policies

Businesses that used information technology were asked to identify whether they had used incident response computer security policies, including:

- *use of incident response team*: the use of consultants, not comprised of employees of a business, to investigate and respond to computer security incidents
- *business continuity plan*: policies that allow a business to conduct its normal operations in the event of computer systems being non-operational
- *forensic plans*: policies that govern preservation of digital evidence following a computer security incident



Note: n=3,616. Excludes 307 businesses with no information technology and 77 missing answers (76 from small, 1 from medium businesses)
 Source: AIC, ABACUS 2008 [computer file, weighted data]

- *incident management procedures*: policies that dictate standard procedures for dealing with computer security incidents.

Incident response policies were used by 12 percent of ABACUS respondents (19% of small, 28% of medium, 47% of large businesses). Figure 13 shows businesses' use of incident response policies.

Policies relating to using an incident response team were in place in only two percent of ABACUS respondents' businesses (1% of small, 6% of medium, 8% of large businesses). Thirty percent of respondents to the survey by the Computer Emergency Response Team et al. used incident response team policies.

Five percent of ABACUS respondents who used information technology during the 12-month period ending 30 June 2007 (4% of small, 14% of medium, 26% of large businesses) used a business continuity policy during the same period. This is a considerably smaller proportion of respondents than that found by AusCERT (54%).

Forensic plans were used by fewer than one percent of ABACUS respondents (<1% of small, 1% of medium, 3% of large businesses). Slightly larger proportions of respondents to Quinn's survey (3%) and AusCERT's survey (6%) used forensic plans.

Incident management policies were used by five percent of ABACUS respondents with information technology (4% of small, 12% of medium, 27% of large businesses). Greater proportions of businesses in both the New Zealand survey (57%) and the AusCERT survey (51%) used this type of information technology policy.

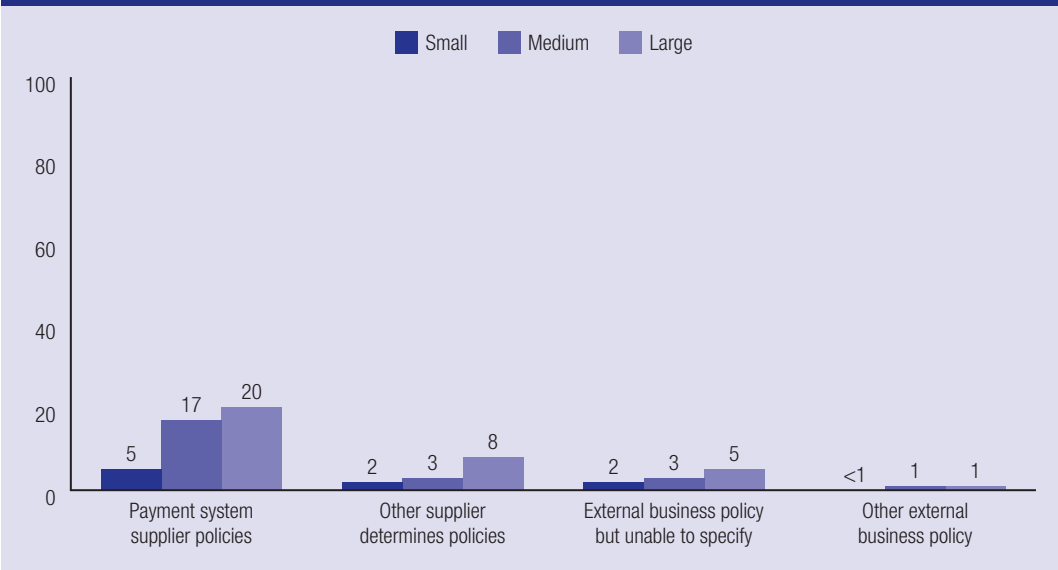
External business computer security policies

Business respondents who indicated they used one or more types of information technology were asked to identify whether their business had used either of the following types of external business policies:

- *payment system supplier policies*: policies that a business is required to follow in order to use an external payment system provider, such as Paypal or credit card payments
- *other supplier determines policies*: policies that a business is required to follow in order to conduct business or use the services of another business.

Nine percent of businesses with information technology (8% of small, 21% of medium, 27% of large businesses) used one or more external

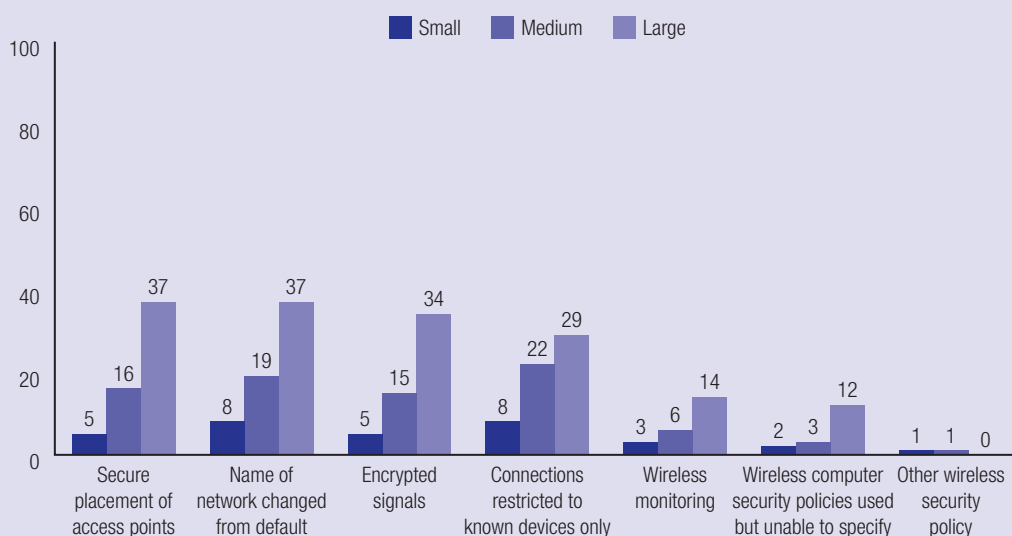
Figure 14 Businesses' use of external business policies, by business size (percent)



Note: n=3,616. Excludes 307 businesses with no information technology and 77 missing answers (76 from small, 1 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Figure 15 Businesses' use of wireless security policies, by business size (percent)



Note: n=3,616. Excludes 307 businesses with no information technology and 77 missing answers (76 from small, 1 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

business policies during the 12-month period ending 30 June 2007. Figure 14 shows the proportions of businesses that used each type of external business policy.

Six percent of respondents (5% of small, 17% of medium, 20% of large businesses) used payment system supplier policies. Just two percent (2% of small, 3% of medium, 8% of large businesses) used policies determined by another supplier. Two percent (2% of small, 3% of medium, 5% of large businesses) of respondents used one or more external business policies, but were unable to specify which policies they had used. Previous research studies on computer security incidents against businesses have not included external business policies in their surveys.

Wireless computer security policies

Finally, business respondents with information technology were asked whether their business had used wireless computer security policies, including:

- *secure placement of access points*: placement of wireless access points in a secure location, such as ceiling or on a high wall

- *name of network changed from default*: changing the default (original) name of the network to a unique name
- *encrypted signals*: signals sent by both wireless hosts and connecting devices in an encrypted format
- *connections restricted to known devices only*: only hardware devices that have been 'set up' as part of the wireless network are able to access the network
- *wireless monitoring*: monitoring content that is sent and received by a wireless device.

Seventeen percent of respondents to the ABACUS survey reported that their businesses had used one or more wireless security policies during the 12-month period ending 30 June 2007 (15% of small, 36% of medium, 56% of large businesses). Figure 15 shows the proportions of businesses that used each type of wireless security policy.

Six percent of businesses with information technology (5% of small, 16% of medium, 37% of large businesses) used secure placement of access points. Nine percent changed the name of their business's network from the default name (8% of small, 19% of medium, 37% of large businesses). Policies related to the use of encrypted signals were

used by seven percent of respondents (5% of small, 15% of medium, 34% of large businesses). Ten percent of businesses (8% of small, 22% of medium, 29% of large businesses) restricted their connections to known devices only. Wireless monitoring policies were used by three percent of businesses overall (3% of small, 6% of medium, 14% of large businesses). Previous research studies on computer security incidents against businesses have not included wireless security policies in their surveys.

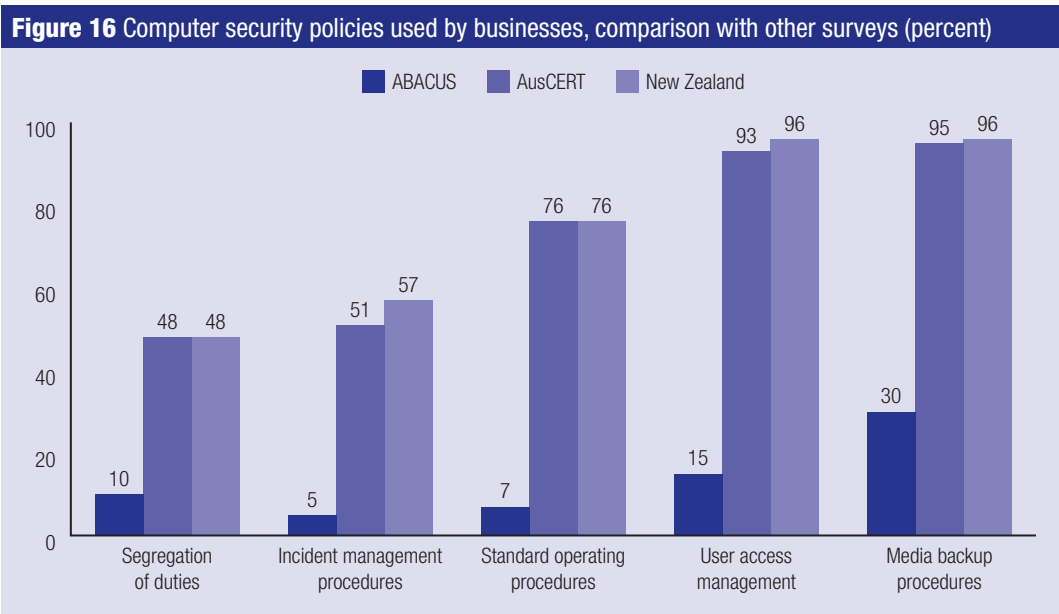
Key findings on businesses' use of computer security policies

The ABACUS data clearly demonstrate that a relationship exists between business size and the use of information technology security policies. Higher proportions of large businesses than medium businesses and higher proportions of medium businesses than small businesses reporting using every computer security policy listed in the ABACUS survey.

Where comparable data exist from previous surveys, smaller (usually significantly smaller) proportions of ABACUS respondents report using each listed computer security policy than do respondents to other surveys (see Figure 16). This may be the case for a variety of reasons, many of which have been outlined above in relation to businesses' use of computer security tools (see pages 43–44).

In addition to these potential explanations, it is important to note that small businesses' low levels of usage of staff/user related policies may have impacted this discrepancy in findings. Due to its representative sample of businesses, most ABACUS respondents were from small businesses, and many are likely to be sole traders. Unlike many previous surveys on computer security incidents against businesses, therefore, a significant proportion of businesses in the ABACUS survey may not have any staff. This may partially explain the small proportions of small businesses reporting having staff/user related policies in place.

The ABACUS data show significantly smaller proportions of computer security tools and policies being used by businesses *and* smaller proportions of businesses experiencing computer security incidents than other surveys have shown previously. There are



Note: ABACUS n=3,616. AusCERT n=389. New Zealand n=113. Excludes 307 businesses with no information technology and 77 missing answers
Source: AIC, ABACUS 2008 [computer file, weighted data]

a number of potential explanations for this discrepancy in findings. Where previous research studies have surveyed the ‘computer security community’ exclusively, or have drawn a sample that disproportionately features members of this community, a number of scenarios are possible.

First, it is possible that businesses belonging to the ‘computer security community’ are targeted by offenders at a much greater rate than businesses belonging to other industries. As such, although the computer security community may have greater levels of protection in place (in the form of computer security tools and/or policies), they may still be experiencing higher levels of computer security incidents. In this scenario, these businesses suffer high levels of computer security incidents *in spite* of the protections they have in place.

It is also possible, however, that businesses belonging to the computer security community experience high levels of security incidents *because* they have sound protections in place. That is, these respondents may simply be more aware of the levels of security incidents that affect their businesses. Although it could be said that these respondents belong to an industry that has much to gain from reporting high levels of computer security incidents, this industry also has much to gain from demonstrating the preventative potential of computer security tools. As such, one would expect to find respondents from the ‘computer security community’ to report either high levels of protection and low levels of security incidents or low levels of protection and high levels of security incidents.

Interestingly, small numbers of respondents reported that using Macintosh computers instead of IBM compatible computers and Linux instead of Windows operating systems formed part of their businesses’ computer security strategies. Small numbers also reported avoiding using wireless technologies and/or the internet in order to avoid computer security incidents. Respondents were not asked direct questions on these topics, however, a number offered these responses when asked about ‘other’ computer security tools and policies used.

Businesses’ use of information technology standards

Table 11 Use of information technology standards in the development of computer security policies, by business size (percent)

	Small	Medium	Large	Weighted n
AS/NZS ISO/IEC 17799:2005 Code of practice for information security management	3	5	15	29
AS/BS7799.2:2003 Information security management	1	2	4	14
ACSI 33 Australian Government Information Security Manual	1	2	5	10
HB 231 2003 Information Security Risk Management	1	1	8	9
HB 171:2003 Guidelines for management of IT evidence	<1	2	2	3
RFC 2196 Site security handbook	1	4	<1	9
ISO/IEC 13335 1:2004 Information technology. Guidelines for the management of IT security	2	4	15	19
State government IT Security standard	1	2	7	13
Other	3	5	3	30

Note: n=1,533. Excludes 307 businesses with no information technology, 2,038 businesses that did not have any information technology standards in place and 123 missing answers (111 from small, 10 from medium, 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Seven percent of ABACUS respondents (7% of small, 10% of medium, 25% of large businesses) with computer security policies in place reported that information technology standards had been used in the development of these policies. Forty percent of businesses overall (38% of small, 48% of medium, 39% of large businesses) reported that they did not know whether any of the information technology standards listed in the ABACUS survey

had been used in the development of computer security policies. As shown in Table 11, large businesses were more likely than medium and small businesses to use almost all of the computer security standards. The most commonly used information technology standards by large businesses were AS/NZS ISO/IEC 17799:2005 and ISO/IEC 13335-1:2004.

Expenditure on computer security

Businesses in the ABACUS study were asked to estimate their total information technology security expenditure for the 2006–07 financial year. As shown in Table 12, the computer security expenditure of businesses varied considerably by business size. The minimum expenditure reported by small, medium and large businesses was \$0, while maximums ranged from \$150,000 for small businesses to \$750,000 for large businesses. As might be expected, the mean expenditure for small businesses (\$992) was smaller than that of medium (\$7,614) and large (\$38,474) businesses. Due to the large proportion of small businesses in the sample, the mean computer security expenditure overall (\$1,830) was closest to the small business mean.

Table 12 Total information technology security expenditure, by business size (\$)				
	Median ^a	Mean	Minimum	Maximum
Small	200	992	0	150,000
Medium	2,000	7,614	0	300,000
Large	10,000	38,474	0	750,000
Businesses overall	250	1,830	0	750,000

a: Medians are only estimates, due to the use of weighted data

Note: n=3,330. Excludes 307 businesses with no information technology and 363 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

The sample of Australian businesses surveyed in the ABACUS study allows an estimate of the total computer security expenditure of businesses to be made. The sample was large enough to provide representative data, and was weighted to accurately reflect the composition of the Australian business

population. Data collected from the ABACUS survey can therefore be multiplied out to produce a weighted estimate of the computer security expenditure of all Australian businesses.

Providing an estimate of the total computer security expenditure of Australian businesses is nonetheless a challenging task, for two main reasons. First, business respondents to the ABACUS survey were asked to provide a *best estimate* of their computer security expenditure. That businesses provided estimates rather than exact figures will impact the accuracy of an estimate of the expenditure of all Australian businesses. It was important for the ABACUS study to ask for an estimate rather than an exact figure, however, to reduce non-response to this question. Second, there were a high number of missing data for this question, with 363 missing answers. Although a high level of non-response is typical for survey questions that ask respondents for financial information, these missing data are important to consider when calculating an estimate of computer security expenditure for the total population of Australian businesses.

As indicated in Table 13, there are a number of methods of calculating this estimate based on the ABACUS data, which produce estimates ranging from \$1.37b to \$1.95b.

The first method assumes that businesses that did not provide an estimate of their computer security expenditure had a total expenditure of \$0. It is certainly possible that respondents with a \$0 computer security expenditure assumed that leaving the question unanswered was the same as providing an answer of \$0. Using this approach, a \$0 value is substituted as the total expenditure on computer security measures for all non-responding businesses. This method of calculating an estimate of Australian businesses' computer security expenditure produces the most conservative estimate of \$1.37b (see Table 13). This same estimate is obtained when calculating total information technology security expenditure across all Australian businesses, excluding those that did not provide an answer to this question.

The second method substitutes the *mean* computer security expenditure of businesses that provided an answer for those that did not. In this method, the mean of \$1,830 is substituted for all businesses that did not provide an estimate of their computer

security expenditure. This mean is based only on the estimates given by respondents to the question. That is, it excludes all non-respondents. This method produces an estimate of \$1.95b (see Table 13).

The third method substitutes the median computer security expenditure of businesses that provided an answer for those that did not. The unweighted median computer security expenditure of \$300 is therefore substituted as the expenditure for all non-respondents to this question. This method produces an estimated total computer security expenditure across all Australian businesses of \$1.42b. It is important to note that due to the skewed nature of the ABACUS data on this variable, the *median* is a more robust measure of central tendency than the *mean*.

The final method used to estimate the total computer security expenditure of Australian businesses was to substitute a predicted value for non-respondents based on industry sector and business size. This method involved using a binomial regression analysis to predict non-respondents' computer security expenditure based on their industry sector and business size. Rather than substituting the *same* measure of central tendency (mean or median) for each non-responding business, this approach calculated a *unique* estimate for each non-responding business. These estimates used the businesses' industry sector and number of employees to predict an approximate value for their computer security expenditure. This method, which takes into account the characteristics of non-respondents and the likely effects of these characteristics on their computer security expenditure, produces the most robust estimate of the total computer security expenditure of all Australian businesses. The estimate, based on this method, is \$1.74b.

Table 13 Estimated total information technology security expenditure across all Australian businesses (\$)

	Estimate 1	Estimate 2	Estimate 3	Estimate 4
Small	671m	1.2b	710m	802m
Medium	516m	588m	522m	671m
Large	184m	191m	185m	272m
Business overall	1.37b	1.95b	1.42b	1.74b

Source: AIC, ABACUS 2008 [computer file, weighted data]

Businesses from each industry sector also reported a minimum computer security expenditure of \$0. The highest maximum expenditure was reported by the electricity, gas, water and waste services sector (\$750,000) followed by information media and telecommunications (\$400,000). Administrative and support services reported the lowest maximum computer security expenditure, with \$30,000. The highest mean expenditure was reported by the electricity, gas, water and waste services (\$6,354) and information media and telecommunications (\$5,374) sectors (see Table 14).

The four methods used to estimate the total information technology security expenditure of Australian businesses for the 2006–07 period were also used to calculate an estimate of expenditure by industry sector. Table 15 shows the four estimates calculated for each industry sector. As discussed, the fourth estimate, which uses a predicted value for each non-responding business, is the most robust.

Businesses that used information technology were asked to indicate whether their business's spending on computer security measures had increased, decreased or stayed the same during the 12-month period ending 30 June 2007, compared with spending in the previous financial year. Fifty-eight percent of these respondents indicated that computer security spending had stayed the same, 18 percent that spending had increased and two percent that it had decreased. Twenty-two percent of respondents did not know whether their business's computer security had increased, decreased or stayed the same in relation to the previous financial year. The proportion of respondents that could not identify whether spending had increased, decreased or stayed the same was quite consistent across business size, with 22 percent of small, 23 percent of medium and 21 percent of large business respondents selecting this option.

These findings differ considerably from the findings of the two other surveys that have asked businesses a similar question. AusCERT (2006: 12), for example, found that 50 percent of respondents had increased computer security spending and 50 percent had not increased spending in the previous year (1% reported not knowing whether spending had increased). Importantly, participants in the AusCERT

Table 14 Total information technology security expenditure, by industry sector (\$)

	Median ^a	Mean	Minimum	Maximum
Agriculture, forestry and fishing	120	898	0	120,000
Mining	500	5,424	0	250,000
Manufacturing	400	2,734	0	200,000
Electricity, gas, water and waste services	200	6,354	0	750,000
Construction	200	692	0	40,000
Wholesale trade	500	2,495	0	80,000
Retail trade	250	1,710	0	100,000
Accommodation and food services	150	1,054	0	100,000
Transport, postal and warehousing	200	1,694	0	250,000
Information media and telecommunications	300	5,374	0	400,000
Financial and insurance services	300	2,584	0	200,000
Rental, hiring and real estate services	300	1,810	0	50,000
Professional, scientific and technical services	500	2,409	0	200,000
Administrative and support services	350	1,812	0	30,000
Public administration and safety	500	1,493	0	100,000
Education and training	300	4,261	0	300,000
Health care and social assistance	300	1,559	0	60,000
Arts and recreational services	177	1,684	0	300,000
Other services	200	1,885	0	50,000
Total	250	1,830	0	750,000

a: Medians are only estimates due to the use of weighted data

Note: n=3,330. Excludes 307 businesses with no information technology and 363 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 15 Estimated total information technology security expenditure across all Australian businesses, by industry sector (\$)

	Estimate 1	Estimate 2	Estimate 3	Estimate 4
Agriculture, forestry and fishing	53.6m	86.2m	56.2m	62.8m
Mining	13.6m	16.9m	13.9	22.3m
Manufacturing	122m	162m	125m	147m
Electricity, gas, water and waste services	13.8m	15.4m	13.9m	16.9m
Construction	73.7m	160m	80.5m	89.9m
Wholesale trade	90.7m	117m	92.7m	118m
Retail trade	119m	179m	124m	153m
Accommodation and food services	48.2m	93.2m	51.8m	68.0m
Transport, postal and warehousing	59.6m	90.5m	62.0m	67.6m
Information media and telecommunications	35.9m	40.9m	36.3m	47.6m
Financial and insurance services	157m	196m	160m	202m
Rental, hiring and real estate services	52.3m	72.6m	53.9m	70.1m
Professional, scientific and technical services	246m	290m	249m	306m
Administrative and support services	57.5m	82.4m	59.5m	85.4m
Public administration and safety	4.8m	7.6m	5.0m	7.0m
Education and training	48.3m	59.6m	49.2m	57.2m
Health care and social assistance	69.3m	104m	72.0m	93.8m
Arts and recreational services	17.2m	28.5m	18.1m	22.0m
Other services	89.2m	145m	93.6m	109m
Total	1.37b	1.95b	1.42b	1.74b

Note: n=3,330. Excludes 307 businesses with no information technology and 363 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

study were asked whether their business's spending had increased *due to concerns about the adequacy of computer security within your organisation*. This constrains responses in a different way from the ABACUS survey. For example, participants in AusCERT's research may have answered 'no' in response to this question if their business's computer security spending had increased for a reason other than concerns about the adequacy of security. Additionally, it is unknown whether the 50 percent of AusCERT respondents that did not increase computer security spending decreased spending or did not change their level of spending. Forty-three percent of respondents to the Department of Trade and Industry's survey reported that their information technology security expenditure had increased in the previous year and two percent reported that it had decreased. It is unclear, however, whether the expenditure of the remaining 55 percent of businesses remained the same.

Expenditure on computer security tools

Respondents were asked to estimate the percentage of their business's information technology security budget that was spent on physical security, cryptographic and authentication tools, anti-fraud and malware tools, detection and monitoring tools, security management technologies and other tools. In general, businesses reported making greater investments in anti-fraud and malware tools and detection and monitoring tools than the other categories. This is consistent with businesses' high levels of use of anti-spam, anti-virus and anti-spyware software, and intrusion detection and intrusion prevention systems. Large businesses also reported investing considerable proportions of their information technology budgets in security management tools. Consistently high proportions of small, medium and large businesses did not know what proportion of information technology security expenditure their business had directed towards each of these types of security tools.

Table 16 shows businesses' expenditure on physical security measures. Overall, a higher proportion of medium businesses (30%) reported some expenditure on physical security than large (24%) or small businesses (17%). Although higher proportions of small (46%) than medium (31%) or large (23%) businesses reported spending zero percent of their information technology security budget on physical security measures. This suggests that there is no direct relationship between business size and expenditure on physical security measures.

Table 16 Expenditure on physical computer security (percent)				
	Small	Medium	Large	Weighted n
0	46	31	23	1,442
>0 – <10	1	3	6	42
10–24	6	10	20	198
25–49	2	6	9	70
50–74	4	6	5	123
75–100	4	5	4	129
Don't know	38	40	33	1,233
Total	100	100	100	3,237

Note: Excludes 307 businesses with no information technology and 457 missing answers (420 from small, 32 from medium, 4 from large businesses)
Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 17 shows the proportion of businesses' information technology budgets spent on cryptographic and authentication tools. A relationship exists between business size and expenditure on cryptographic and authentication tools, with a higher proportion of large than medium businesses, and a higher proportion of medium than small businesses reporting some expenditure on this type of computer security tool. Thirty-three percent of large businesses, compared with 14 percent of medium and eight percent of small businesses directed a proportion of their spending towards cryptographic and authentication measures. Smaller proportions of large businesses (35%) than medium (46%) or small (53%) businesses reported spending zero percent of their information technology budget on this category of security tool.

Table 17 Expenditure on cryptographic and authentication tools (percent)

	Small	Medium	Large	Weighted n
0	53	46	35	1,697
>0 – <10	1	2	4	46
10–24	4	7	20	145
25–49	1	3	4	41
50–74	1	1	4	25
75–100	1	1	1	20
Don't know	39	41	32	1,263
Total	100	100	100	3,237

Note: Excludes 307 businesses with no information technology and 457 missing answers (420 from small, 32 from medium, 4 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Small, medium and large businesses reported directing higher proportions of their information technology security budgets towards anti-fraud and malware tools than any of the other broad categories of computer security tools. As shown in Table 18, 34 percent of small, 38 percent of medium and 50 percent of large businesses spent some proportion of their computer security budget on anti-fraud and malware tools. As stated previously, this is consistent with businesses' high levels of use of anti-spam, anti-virus and anti-spyware software. Interestingly, however, 31 percent of small, 20 percent of medium and 18 percent of large businesses reported no expenditure on anti-fraud and malware tools. This is somewhat inconsistent with the high proportion of ABACUS respondents that reported using anti-fraud and malware tools. This may suggest that businesses do not view security tools such as anti-virus software, which may be able to be downloaded without cost and are typically included in installation media, as impacting on information technology expenditure.

There also appears to be a direct relationship between business size and expenditure on detection and monitoring computer security tools. A higher proportion of large businesses (50%), than medium (36%) or small (29%) businesses reported some expenditure on detection and monitoring tools. Conversely, a larger proportion of small businesses (35%) than medium (22%) or large (18%) businesses reported \$0 expenditure on this type of computer security tool (see Table 19).

Table 18 Expenditure on anti-fraud and malware tools (percent)

	Small	Medium	Large	Weighted n
0	30	20	18	929
>0 – <10	1	2	3	40
10–24	5	8	24	169
25–49	5	9	11	164
50–74	8	8	7	248
75–100	15	11	5	468
Don't know	37	41	32	1,218
Total	100	100	100	3,237

Note: Excludes 307 businesses with no information technology and 457 missing answers (420 from small, 32 from medium, 4 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 19 Expenditure on detection and monitoring tools (percent)

	Small	Medium	Large	Weighted n
0	35	22	18	1,070
>0 – <10	2	2	2	53
10–24	5	11	25	187
25–49	5	9	15	175
50–74	7	8	4	227
75–100	10	6	4	301
Don't know	37	41	32	1,224
Total	100	100	100	3,237

Note: Excludes 307 businesses with no information technology and 457 missing answers (420 from small, 32 from medium, 4 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

A similar relationship exists between business size and expenditure on security management tools, with 45 percent of large businesses, compared with 28 percent of medium businesses and 14 percent of small businesses reporting expending some of their computer security budget on security management tools. As shown in Table 20, it was again found to be the case that a higher proportion of small than medium businesses and a higher proportion of medium than large businesses reported \$0 expenditure on security management tools.

Table 20 Expenditure on security management tools (percent)

	Small	Medium	Large	Weighted n
0	48	33	24	1,492
>0 – <10	1	2	2	43
10–24	4	10	22	154
25–49	3	8	10	113
50–74	3	4	9	96
75–100	3	4	2	100
Don't know	38	40	32	1,238
Total	100	100	100	3,237

Note: Excludes 307 businesses with no information technology and 457 missing answers (420 from small, 32 from medium, 4 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Evaluation of computer security

ABACUS respondents with computer security measures in place were asked to identify which method(s) their business had used to evaluate its computer security during the 12-month period to 30 June 2007. Businesses were asked about:

- *security audits by internal staff*: a measurable technical assessment of a network, system or application that is carried out by a staff member of the business
- *security audits by external businesses*: a measurable technical assessment of a network, system or application that is carried out by a person who is not a staff member of the business
- *security compliance checks*: assessments used to check security issues in terms of their compliance with a policy
- *automated tools*: software that monitors and reports on the status of files and settings on systems, networks, and/or servers
- *email monitoring software*: software that is designed to monitor the email activity of users
- *web activity monitoring software*: software that is designed to monitor the web activity of a specific user or users.

Of those businesses that evaluated their information technology security during the 12-month period ending 30 June 2007 (24%), 32 percent used a security audit by internal staff, 31 percent email monitoring software, 27 percent automated tools, 22 percent web activity monitoring software and 21 percent security audits by external organisations. Table 21 shows the proportions of small, medium and large businesses that used each of these methods of evaluation. Security audits by internal staff and email monitoring software were the methods of evaluation used by the highest proportion of small and medium businesses. For large businesses, email monitoring software and security audits by internal staff were the most commonly used methods of evaluating computer security. Importantly, 24 percent of respondents did not know which method of computer security evaluation their business had used. A considerable proportion of small (24%), medium (22%) and large (10%) businesses reported not knowing whether or how often their business's computer security was evaluated.

Table 21 Method of evaluation of computer security, by business size (percent)

	Small	Medium	Large	Weighted n
Security audit by internal staff	31	40	51	413
Security audits by external businesses	19	33	45	277
Automated tools	29	20	28	351
Email monitoring software	30	36	51	404
Web activity monitoring software	21	30	42	285
Other	1	1	2	14

Note: n=3,617. Excludes 307 businesses with no information technology and 77 missing answers (69 from small, 8 from medium, fewer than 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Proportions of businesses using each of these methods of evaluating their computer security do not vary greatly. This was also the case in both Richardson's (2007: 19) survey of businesses in the United States and Quinn's (2006) survey of New

Zealand businesses. These surveys reveal, however, much higher proportions of businesses utilising each of these methods of evaluation. Richardson (2007) found that 63 percent of businesses in the United States used security audits by internal staff, 53 percent used penetration testing and security audits by external organisations, 49 percent used automated tools, 45 percent used web activity monitoring software and 44 percent used email monitoring software. Quinn (2006) found that 84 percent of New Zealand businesses used email monitoring software, 79 percent used web activity monitoring software, 72 percent used penetration testing, 64 percent used security audits by internal staff, 53 percent used security audits by external organisations and 46 percent used automated tools.

There are a number of potential explanations for the finding that lower proportions of respondents to the ABACUS survey used each of these methods to evaluate their computer security.

As outlined earlier in this report, Quinn’s (2006) survey in New Zealand targeted businesses identified in previous research by the University of Otago as belonging to the top 500 organisations by turnover. The survey excluded ‘smaller’ businesses (although it does not define these) but included local and national government organisations. Richardson’s (2007) research in the United States focused primarily on members of the Computer Security Institute, including those belonging to local, state and federal government organisations. As will be discussed later in this report, large businesses and businesses with high annual turnovers are more likely to have specialised information technology staff with sound knowledge of, and abilities in, information technology. This is less likely to be the case in small businesses, which comprised the majority of respondents to the ABACUS survey.

Government organisations, which may be more publicly accountable than private organisations, are potentially more likely to have documented procedures in place for evaluating computer security. Businesses that belong to computer security groups and associations, such as those surveyed by Richardson (2007) are likely to have a detailed knowledge of the computer security environment and therefore be familiar with tools and methods for evaluating computer security. These factors may

contribute to the finding that, in contrast to respondents to the New Zealand and US surveys, smaller proportions of ABACUS survey respondents used each of the methods of computer security evaluation.

Table 22 shows the frequency of evaluation of small, medium and large businesses’ computer security. Twenty percent of businesses (19% of small, 27% of medium, 43% of large businesses) reported evaluating their computer security during the 12-month period to 30 June 2007.

Table 22 Frequency of evaluation of computer security measures, by business size (percent)				
	Small	Medium	Large	Weighted n
Daily	1	2	2	49
Weekly	2	3	<1	75
Monthly	5	7	6	173
Quarterly	3	5	9	111
Biannually	3	4	11	124
Annually	3	5	9	130
Ad hoc	<1	1	3	12
Other	1	1	2	39
Don't know	16	21	23	596
Not evaluated	65	52	34	2,305
Total	100	100	100	3,617

Note: Excludes 307 businesses with no information technology and 77 missing answers (69 from small, 8 from medium, fewer than 1 from large businesses)
Source: AIC, ABACUS 2008 [computer file, weighted data]

Where businesses have evaluated their computer security during the 12-month period, a relatively even distribution can be seen across the *monthly*, *quarterly*, *biannually* and *annually* categories, with small and medium businesses most likely to evaluate their computer security monthly, and large businesses most likely to evaluate their computer security biannually.

Outsourcing

In recent years, the tendency of businesses to minimise costs by locating some of their operations in developing countries with cheaper labour costs

has resulted in an increasing number of business functions being conducted from outside of Australia (Choo, Smith & McCusker 2007a: 22). In the ABACUS survey, of those businesses that reported using some type of information technology, 19 percent reported outsourcing some computer security measures to one or more third parties, either within Australia or overseas. Table 23 shows the proportions of small, medium and large businesses that outsourced one or more security measures. Of those that outsourced computer security measures, 15 percent reported outsourcing to one or more third parties based in a country other than Australia (Table 24). Of those that outsourced computer security measures, 66 percent (63% of small, 76% of both medium and large businesses) reported evaluating their outsourced measures during the reporting period (see Table 25).

Table 23 Outsourcing of computer security measures, by business size (percent)				
	Small	Medium	Large	Weighted n
Outsource	17	38	42	710
Don't outsource	78	56	52	2,747
Don't know	6	5	6	200
Total	100	100	100	3,658

Note: Excludes 307 businesses with no information technology and 36 missing answers (36 from small, fewer than 1 from medium businesses)
Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 24 Offshoring of computer security measures, by business size (percent)				
	Small	Medium	Large	Weighted n
Offshore	15	11	31	102
Don't offshore	80	87	68	563
Don't know	5	2	<1	28
Total	100	100	100	693

Note: Excludes 307 businesses with no information technology, 2,747 businesses that did not outsource any computer security measures, 200 businesses that did not know whether they had outsourced any computer security measures, 18 missing answers (12 from small, 5 from medium, fewer than 1 from large businesses) and 36 missing answers from the previous question about outsourcing
Source: AIC, ABACUS 2008 [computer file, weighted data]

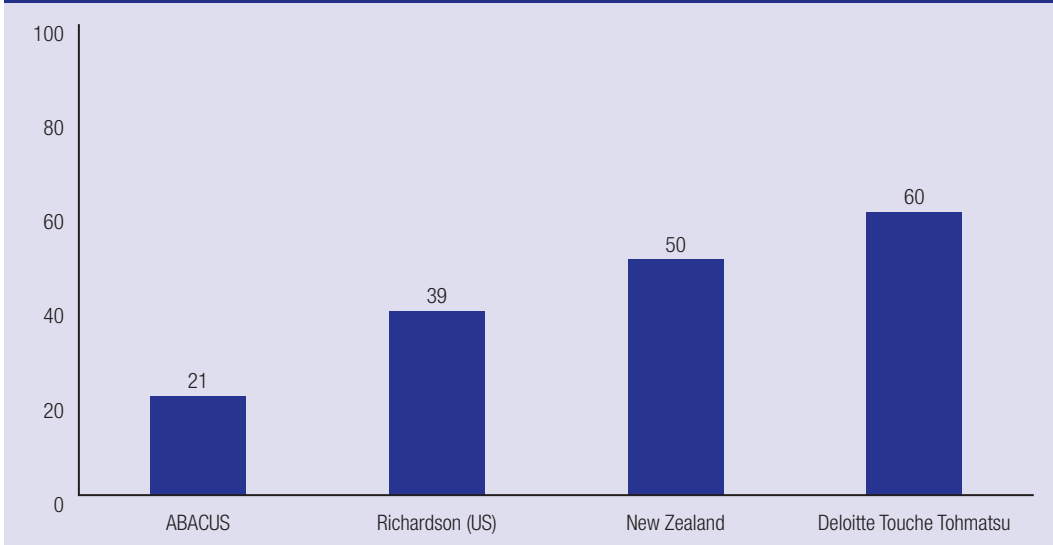
The ABACUS data on outsourcing computer security functions vary considerably from those

of other surveys on computer security incidents against businesses. The ABACUS survey found that only 19 percent of businesses outsourced any computer security function to one or more third parties during the 12-month period ending 30 June 2007. As Figure 17 shows, this is a lower proportion than that found by existing surveys on computer security incidents against businesses. There are a number of potential explanations for this difference in findings among surveys.

- The lower proportion of businesses that reported outsourcing computer security measures in the ABACUS survey may reflect the representativeness of the survey. The higher proportion of small businesses in the ABACUS sample—in line with the proportion of small businesses in Australia—may have impacted on this finding. Small businesses may simply lack the information technology security infrastructure to warrant outsourcing. Many small businesses reported having only rudimentary computer security tools, such as anti-virus software, in place.
- Larger businesses and businesses with higher annual turnovers, which were disproportionately sampled in many previous surveys, are likely to have more involved information technology security measures in place. Outsourcing these measures may therefore result in considerable fiscal savings for these businesses. This is unlikely to be the case for small businesses, which form the majority of the ABACUS sample.
- Cultural differences may also have contributed towards the diverse findings from surveys on computer security incidents against businesses.

Table 25 indicates the methods used by businesses to evaluate their outsourced computer security. Small and medium businesses were most likely to use security audits by internal staff in order to evaluate their outsourced security measures, followed by security audits by external businesses. Large businesses were most likely to use security audits by external parties, followed by security audits by internal staff. This may reflect, in part, the greater information technology security budgets of large businesses.

Figure 17 Businesses that outsourced one or more computer security measure, comparison with other surveys (percent)



Note: ABACUS n=3,658. Excludes 307 businesses with no information technology and 36 missing answers (36 from small, fewer than 1 from medium businesses). Richardson n=479. New Zealand n=112. Deloitte Touche Tohmatsu n=unknown

Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 25 Method of evaluation of outsourced computer security, by business size (percent)

	Small	Medium	Large	Weighted n
Security audit by internal staff	25	36	28	170
Security audits by external businesses	20	26	35	136
Security compliance check	11	13	20	73
Other	6	2	5	29
Third party performance was evaluated but unable to specify	26	22	26	176

Note: n=696. Excludes 307 businesses with no information technology, 2,747 businesses that did not outsource any computer security measures, 200 businesses that did not know whether any computer security measures had been outsourced, 36 missing answers from the previous question about outsourcing and 14 missing answers (12 from small, 2 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 26 indicates the frequency of evaluation of outsourced computer security measures by small, medium and large businesses. It shows that small and medium businesses were most likely to evaluate outsourced computer security measures on a

monthly or ad hoc basis, and large businesses were most likely to evaluate outsourced security measures on an ad hoc or quarterly basis.

Table 26 Frequency of evaluation of outsourced computer security measures, by business size (percent)

	Small	Medium	Large	Weighted n
Daily	1	0	0	3
Weekly	8	17	10	45
Monthly	22	19	17	95
Quarterly	15	15	19	66
Biannually	7	6	17	31
Annually	11	14	9	52
Ad hoc	22	18	21	96
Other	2	0	0	5
Don't know	14	11	7	59
Total	100	100	100	452

Note: Excludes 307 businesses with no information technology, 2,747 businesses that did not outsource any computer security measures, 200 businesses that did not know whether any computer security measures had been outsourced, 234 businesses that did not evaluate outsourced computer security measures, 36 missing answers from the previous question about outsourcing and 24 missing answers (21 from small, 3 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Insuring against computer security incidents

ABACUS respondents with information technology were asked to identify which types of computer security incidents were covered by their business's insurance policy. Businesses were asked about:

- *insider abuse of access*: when an employee or person authorised to use a business's computer system abuses this access. For example, by accessing the internet for personal use against the business's policy
- *theft or loss of hardware*: when hardware, such as laptops, Personal Digital Assistants or other devices are lost or stolen and not recovered
- *virus or other malicious code*: software designed specifically to damage or disrupt a system. These may be either self-replicating or non self-replicating and work to change the way a computer operates without the consent of the system owner or user
- *spyware*: software designed to secretly collect information from a computer and send it elsewhere or change settings and interfere with the performance of a compromised computer
- *phishing*: assuming the identity of a legitimate business using forged email or fraudulent websites to persuade others to provide information, such as credit card numbers, for the purpose of using it to commit fraud
- *denial of service attacks*: attacks aimed at a specific website by flooding the web server with repeated messages, depleting the system resources and denying access to legitimate users
- *sabotage of network or data*: intentional destruction of, or damage to, a computer network or to data stored on a network or stand alone computer
- *unauthorised network access*: obtaining access to a restricted computer network without providing adequate credentials such as logon name and password
- *theft or breach of proprietary or confidential information*: unauthorised access to and/or use, viewing, duplication, distribution or theft of information relating to this business's product(s) or activities, such as financial information

- *incidents involving a business's web application*: any malicious or destructive incident that involves a business's website.

The ABACUS survey found that 61 percent of businesses with information technology had an insurance policy that covered one or more computer security incidents. The remaining 39 percent either were not covered for one or more types of computer security incidents or did not know the extent of their insurance coverage in relation to computer security incidents. Fifty-nine percent of small businesses, 80 percent of medium businesses and 88 percent of large businesses with some type of information technology had an insurance policy that covered at least one type of computer security incident during the reporting period. As indicated in Table 27, considerable proportions of respondents from small (33%), medium (40%) and large (49%) businesses did not know whether any types of the computer security incidents listed in the ABACUS survey were covered by their business's insurance policy.

Of businesses utilising some form of information technology, the type of computer security incident most likely to be covered by an insurance policy was theft or loss of hardware. This was the case for small, medium and large businesses. This is perhaps unsurprising, given that this category of computer security incident is related most closely to traditional larceny offences. Across the three business sizes, viruses and other malicious code were also likely to be insured against, although for medium businesses, theft or loss of hardware was followed by insider abuse of access.

Higher proportions of ABACUS respondents reported having an insurance policy that covered computer security incidents than has been found in comparable international surveys. Richardson's (2007) research in the United States found that 29 percent of respondents had an insurance policy that covered computer security risks, and Quinn's (2006) research in New Zealand found that just 16 percent of businesses had the same. This is a surprising finding, given that as outlined above, Richardson's survey focused on members of the Computer Security Institute, including government organisations, and Quinn's research excluded small businesses and included government organisations. It might be expected that a higher proportion of

respondents to these surveys would have insurance policies that cover computer security incidents.

Table 27 Computer security incidents covered by insurance policies, by business size (percent)				
	Small	Medium	Large	Weighted n
Insider abuse of access	3	13	13	141
Theft or loss of hardware	18	35	29	728
Virus or other malicious code	8	12	16	312
Spyware	7	11	12	279
Phishing	3	5	7	121
Denial of service attack	1	3	2	28
Sabotage of network or data	2	9	12	104
Unauthorised network access	3	9	14	141
Theft or breach of proprietary or confidential information	4	11	12	171
Incident involving the business's web application	1	2	2	27
Other	1	1	<1	29

Note: n=3,594. Excludes 307 businesses with no information technology and 99 missing answers (88 from small, 9 from medium, 2 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

As stated above, theft or loss of hardware was identified as the most common computer security incident covered by businesses’ insurance policies by the highest proportion of small (18%), medium (35%) and large (29%) businesses. This computer security incident is perhaps the most likely to be viewed by respondents as a traditional, ‘terrestrial’ offence and may therefore be more likely to be covered by businesses’ insurance policies. This is one potential explanation for the higher proportion of business respondents to the ABACUS survey reporting that they have cyber insurance.

Computer security awareness-raising initiatives

Respondents were asked to identify whether they were familiar with a range of awareness-raising initiatives related to computer security. Awareness-raising initiatives included in the survey were:

- *Stay Smart Online*: an Australian Government initiative aimed at improving home and small business users’ computer security
- *Scamwatch*: an Australian Competition and Consumer Commission program that provides information to consumers and small businesses on how to avoid scams, including internet scams
- *FIDO*: an Australian Securities and Investment Commission initiative aimed at protecting consumers from scams, including internet scams
- *Australian High Tech Crime Centre*: Australia’s national agency for combating high tech crimes
- *AusCERT*: Australia’s national computer emergency response team
- *Stay Safe Online*: a national initiative that provides information to consumers and small businesses on avoiding cybercrimes.

In general, 21 percent of businesses (20% of small, 29% of medium, 51% of large businesses) reported being aware of at least one of these initiatives. Table 28 shows the breakdown of businesses’ familiarity with each awareness-raising initiative. FIDO was the most widely recognised overall, with 11 percent of respondents (11% of small, 15% of medium, 19% of large businesses) reporting familiarity with this initiative. This was followed by Stay Safe Online, which was known to six percent of businesses (6% of small, 7% of medium, 15% of large businesses) in the ABACUS survey.

Table 28 Familiarity with awareness-raising initiatives, by business size (percent)

	Small	Medium	Large	Weighted n
Stay smart online	4	6	10	164
Scamwatch	5	9	8	198
FIDO	11	15	19	392
Australian High Tech Crime Centre	2	3	7	70
AusCERT	2	8	25	105
Stay safe online	6	7	15	204
Other	1	<1	<1	33

Note: n=3,693. Excludes 307 businesses with no information technology and 176 missing answers (153 from small, 22 from medium, 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Importantly, the ABACUS data suggest that 79 percent of businesses are unaware of any of these initiatives. A smaller proportion of large businesses (49%) than medium (71%) or small (80%) businesses reported being unaware of any of the initiatives listed in the ABACUS survey.



Prevalence of computer security incidents against Australian businesses

Businesses in the ABACUS survey were asked to indicate how many computer security incidents their business had experienced during the 2006–07 financial year. Findings related to the prevalence of computer security incidents are presented in this section and compared with existing data from previous surveys where possible.

Number of computer security incidents experienced

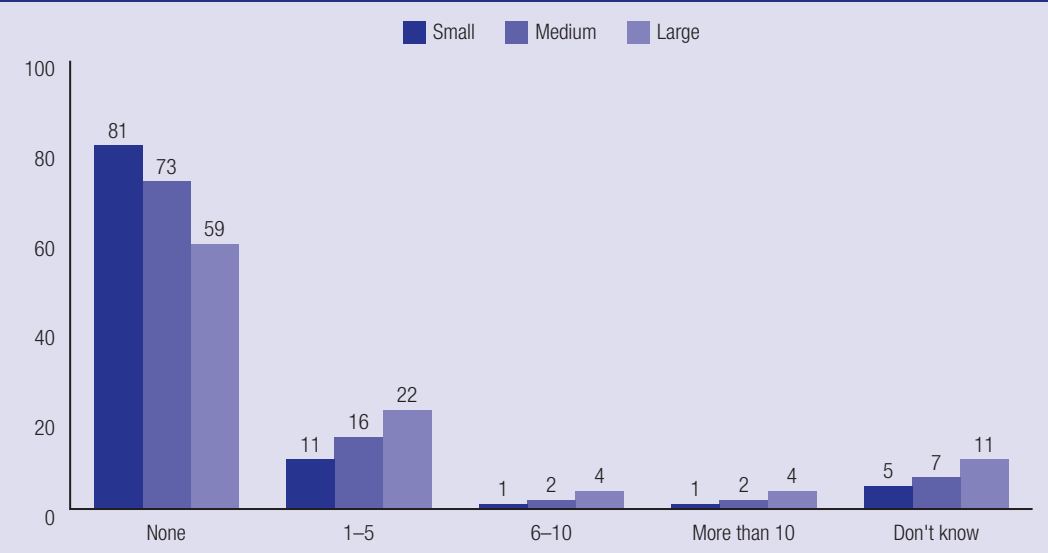
A majority of businesses (80%) that used information technology reported experiencing no computer security incidents during the 12-month period ending on 30 June 2007. The ABACUS data show that as a proportion of the overall sample, 12 percent of businesses experienced one to five computer security incidents, one percent experienced six to 10 incidents and one percent more than 10 incidents. Six percent of respondents were unable to quantify the number of computer security incidents their business had experienced (see Figure 18).

These findings closely reflect those of both AusCERT (2006) and the ABS (2007), but vary considerably

from Richardson's (2007) and Rantala's (2008) US study. A higher proportion of respondents to Richardson's (46%) and Rantala's (67%) surveys reported experiencing one or more computer security incidents than they did in either the ABACUS or AusCERT surveys. There are a number of potential explanations for this:

- Richardson's survey sampled computer security professionals from businesses affiliated in some way with the Computer Security Institute. These respondents are probably more knowledgeable about computer security incidents and better able to identify a computer security incident than members of the broader business community. As such, these respondents may simply be more aware of computer security incidents that take place. Respondents from outside the computer security industry may view some computer security incidents in technical terms ('the computer crashed') rather than in criminal terms. Conversely, businesses with limited information technology capacity, drawn from the broader business population, may lack awareness of and therefore under-report, computer security incidents. Additionally, limited information technology infrastructure, particularly among small businesses, may result in the reduced likelihood of businesses correctly identifying computer security incidents.

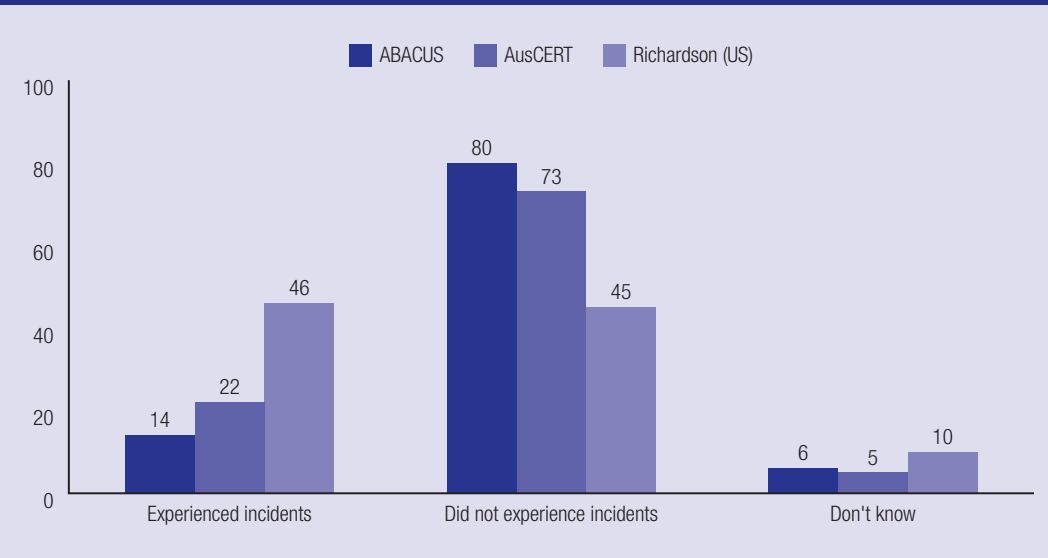
Figure 18 Number of computer security incidents experienced, by business size (percent)



Note: n=3,620. Excludes 307 businesses with no information technology and 74 missing answers (61 from small, 12 from medium, 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Figure 19 Whether any computer security incidents experienced, comparison with other surveys (percent)

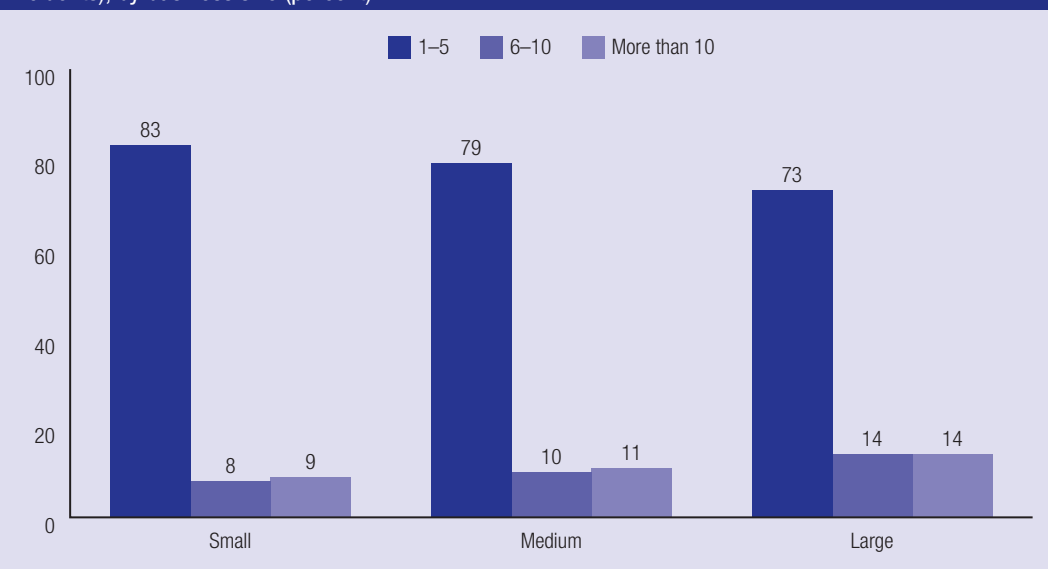


Note: ABACUS n=3,620. Excludes 307 businesses with no information technology and 74 missing answers. AusCERT n=389. Richardson n=487

Source: AIC, ABACUS 2008 [computer file, weighted data]

- It is important to note, however, that a lower proportion of respondents to the ABACUS survey (6%) than to Richardson's survey (23%) reported not knowing how many computer security incidents their organisation had experienced in the preceding 12 months.
- It may also be the case that businesses in the United States are victimised by more computer security incidents than Australian businesses. As previously stated, Symantec (2007: 30) have reported that most of the world's malicious activity originates in the United States. IBM Global

Figure 20 Number of computer security incidents experienced (among businesses experiencing incidents), by business size (percent)



Note: n=527. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience a computer security incident, 212 don't know responses and 74 missing answers (61 from small, 12 from medium, 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Technology Services (2008) similarly report that the United States is the origin of more spam, spam URLs, phishing URLs and overall criminal content than any other country.

Of those businesses that were able to identify the number of computer security incidents experienced, 83 percent (83% of small, 8% of medium, 9% of large businesses) reported experiencing one to five computer security incidents, eight percent (79% of small, 10% of medium, 73% of large businesses) six to 10 incidents and nine percent (73% of small, 14% of medium and large businesses) more than 10 incidents (see Figure 20).

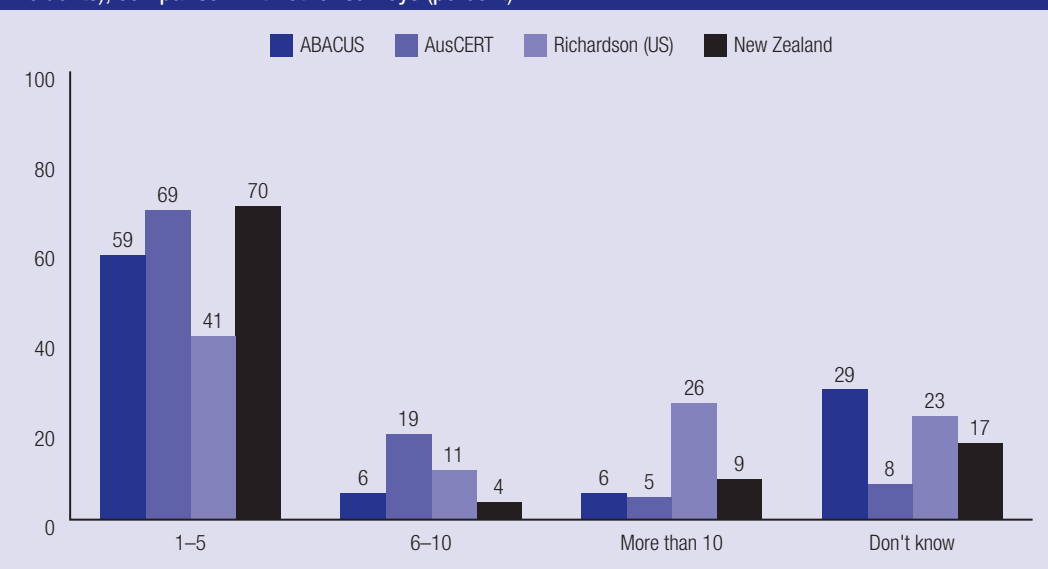
Figure 20 shows the number of computer security incidents reported by businesses that had experienced one or more computer security incidents in comparison with previous surveys. As stated previously, 12 percent of ABACUS respondents overall experienced one to five computer security incidents. AusCERT's survey found that a similar proportion of total respondents (15%) had experienced one to five incidents. These data contrast with those from the US survey by the Computer Emergency Response Team et al. (2007), which found that 40 percent of businesses reported

experiencing one to five incidents and 22 percent experienced 10 or more incidents and Rantala's (2008: 4) survey, which found that 43% of businesses detected 10 or more incidents during 2005. This discrepancy in findings may suggest a cultural difference between the United States and the Antipodes in relation to the frequency with which businesses experience computer security incidents.

The UK's Department of Trade and Industry's (2006: 21) survey found that the median number of computer security incidents experienced by businesses was five. Among businesses that had experienced one or more incidents, the median number of incidents was eight. The Computer Emergency Response Team et al. (2007) reported a median of two incidents overall and a median of four incidents among those businesses that had experienced one or more computer security incidents.

The mean number of computer security incidents experienced by ABACUS respondents was seven. The ABACUS survey found an estimated median of zero computer security incidents was experienced by businesses. Small, medium and large businesses all experienced an estimated median of zero

Figure 21 Number of computer security incidents experienced (among businesses experiencing incidents), comparison with other surveys (percent)



Note: ABACUS n=738. Excludes 307 businesses with no information technology, 2,881 businesses that experienced no computer security incidents and 74 missing answers (61 from small, 12 from medium, 1 from large businesses). AusCERT n=86. Richardson n=280. New Zealand n=unknown

Source: AIC, ABACUS 2008 [computer file, weighted data]

incidents. The pronounced difference between the mean number of incidents and the median number of incidents, as well as the very large standard deviation, indicate that the data collected on the number of computer security incidents experienced by businesses are highly skewed. This is due primarily to a small number of businesses reporting very large numbers of computer security incidents. As a result of this skew, the estimated *median* number of computer security incidents, rather than the *mean*, should be considered the more accurate of the two measures of central tendency.

Which business types are more likely to experience computer security incidents?

There are somewhat conflicting views in the existing literature and research on computer security incidents against businesses as to which types of businesses are more likely to experience computer security incidents. Large businesses and businesses from the financial sector are usually thought to be

the most at risk, as they are considered the most 'appealing' targets and more likely to result in financial gain for perpetrators of computer security incidents.

Business size and likelihood of experiencing computer security incidents

The ABACUS survey found that large businesses were less likely than medium or small businesses to report having experienced no computer security incidents, but more likely than medium or small businesses to report having experienced one to five, six to 10 and more than 10 incidents. These data suggest that there is a relationship between business size and the number of incidents experienced by businesses, with large businesses more likely to experience higher levels of computer security incidents. The limited information technology infrastructure of some businesses, including many small businesses, may result in these businesses being less likely to experience a computer security incident.

A number of previous surveys have presented similar results. The Department of Trade and Industry (2006: 21) found that in the United Kingdom, a higher proportion of large businesses than businesses overall reported both computer security incidents in general and ‘malicious computer security incidents’. Rantala (2008: 1) also found a relationship between business size and number of computer security incidents experienced in the United States.

In contrast, results from Hong Kong’s component of the International Crimes Against Businesses survey suggest that businesses with fewer than 100 employees were more likely to have experienced a computer security incident than businesses with 100 or more employees (Broadhurst et al. 2006). The ABACUS data therefore appear to support conclusions different from those of the Hong Kong survey.

Importantly, the ABACUS survey defined business size in relation to the number of employees a business had. Small businesses were defined as those with 0–19 employees, medium businesses as those with 20–199 employees and large businesses as those with 200 or more employees. Other surveys have categorised businesses into sizes according to the annual revenue of the business. Results from the Hong Kong survey suggest that there is a relationship between the annual turnover of businesses and whether businesses had experienced any computer security incidents. Businesses with a higher annual turnover were more likely to experience computer security incidents than those with a lower annual turnover (Broadhurst et al. 2006). As indicated in Table 29,

the ABACUS data also appear to support a relationship between businesses’ annual turnover and the number of computer security incidents experienced. The ABACUS data suggest that smaller proportions of businesses with higher annual turnovers report experiencing no computer security incidents. Eighty-four percent of businesses with an annual turnover of less than \$99,999 reported experiencing no incidents, compared with only 56 percent of businesses with an annual turnover of \$1b or more. Similarly, smaller proportions of businesses that turned over less than \$99,999 (9%) reported experiencing one to five computer security incidents, compared with 30 percent of businesses with a turnover of \$1b or more. This relationship does not appear to exist in relation to greater numbers of computer security incidents experienced (see Table 29).

Industry sector and likelihood of experiencing computer security incidents

It is widely accepted in the literature on computer security incidents against businesses that financial sector organisations are likely targets for perpetrators of computer security incidents. Symantec (2006: 9) state that ‘the financial services industry is a logical target for attackers hoping to profit from attack activity’. There is some evidence to support this view. For example, IBM Global Technology Services (2008) report that 19 out of 20 phishing targets are in the banking industry,

Table 29 Annual turnover, by number of computer security incidents experienced (percent)								
	Less than \$99,999	\$100,000– 499,999	\$500,000– 999,999	\$1m– 9,999,999	\$10m– 99,999,999	\$1b	Don't know	Weighted n
None	84	82	78	76	70	56	78	2,564
1 to 5	9	11	13	15	16	30	18	391
6 to 10	1	1	2	1	2	0	0	42
More than 10	2	1	1	1	3	0	0	44
Don't know	4	5	7	7	9	15	4	188
Total	100	100	100	100	100	100	100	3,229

Note: Excludes 307 businesses with no information technology and 465 missing answers

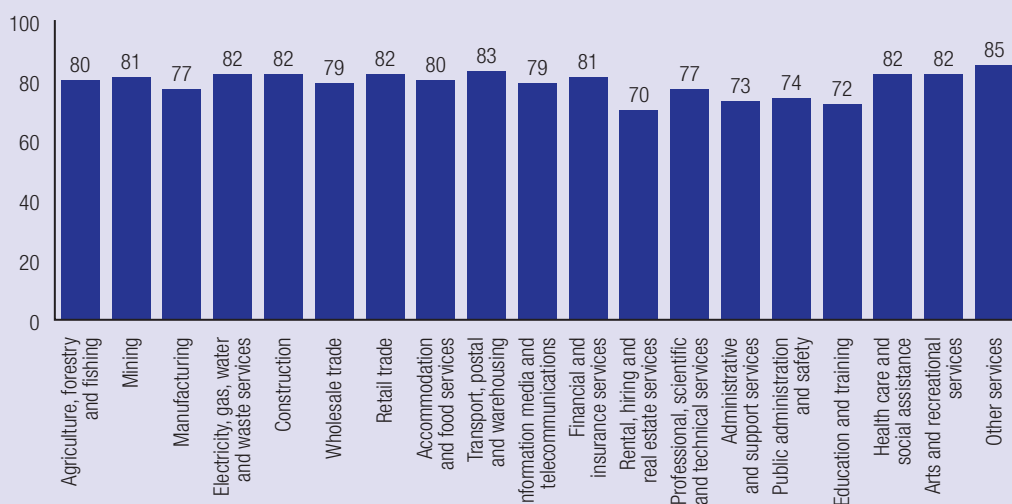
Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 30 Number of computer security incidents experienced, by industry sector (percent)

	None	1–5	6–10	More than 10	Don't know	Weighted n
Agriculture, forestry and fishing	80	12	1	3	5	261
Mining	81	12	1	1	5	14
Manufacturing	77	13	3	<1	7	223
Electricity, gas, water and waste services	82	10	1	<1	7	11
Construction	82	11	1	1	6	531
Wholesale trade	79	13	1	1	6	182
Retail trade	82	10	2	1	5	344
Accommodation and food services	80	11	3	0	6	208
Transport, postal and warehousing	83	13	0	<1	4	168
Information media and telecommunications	79	9	2	1	9	33
Financial and insurance services	81	13	<1	2	4	287
Rental, hiring and real estate services	70	15	2	2	12	135
Professional, scientific and technical services	77	14	1	3	5	482
Administrative and support services	73	20	0	1	6	155
Public administration and safety	74	15	<1	1	10	17
Education and training	72	15	2	1	9	61
Health care and social assistance	82	9	1	2	6	226
Arts and recreational services	82	10	0	1	8	56
Other services	85	7	2	0	7	228

Note: n=3,620. Excludes 307 businesses with no information technology and 74 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

Figure 22 Businesses experiencing no computer security incidents, by sector (percent)

Note: n=3,620. Excludes 307 businesses with no information technology and 74 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

and Symantec (2008: 8) claims that 80 percent of all brands used in phishing attacks are from the financial sector.

In the ABACUS survey, 81 percent of businesses from the financial and insurance services sector that used information technology reported experiencing no computer security incidents, 13 percent experienced one to five incidents, less than one percent six to 10 incidents and two percent more than 10 incidents. These proportions are similar to those of other industry sectors (see Figure 22).

ABACUS data therefore do not strongly support the view that financial organisations are most likely to be the targets of computer security incidents. There are a number of potential explanations for this.

- The view that certain industry sectors are most likely to experience computer security incidents assumes that incidents are targeted rather than random. The ABACUS data indicate, however, that viruses and other malicious code were the most commonly experienced incidents by small, medium and large businesses. Viruses and malicious code may or may not be targeted towards particular businesses or industry sectors. It is also important to note that, of businesses that did not report their most significant computer security incident to a third party, one of the most common reasons provided by small, medium and large businesses was that the business *had not been explicitly targeted*.
- Another potential explanation for this finding is that businesses from sectors outside the financial sector are appealing targets due to the personal data they collect from clients. This may make a variety of other industry sectors appealing targets for perpetrators aiming to commit 'identity theft'. Research by Symantec (2008: 5; 2007: 11) has identified the education and retail/wholesale sectors as frequent targets in this regard. The ABACUS survey, however, did not find higher levels of victimisation among these sectors.
- Businesses from the financial sector may be perceived by cyber criminals as having more stringent information technology security than businesses from other sectors. Financial services organisations may be perceived as having more or 'better' data to protect and therefore as having higher quality security measures in place.

Assuming that computer security incidents are targeted towards specific organisations and/or sectors (although this may not be the case, as discussed previously), this may help explain the finding that businesses from the financial and insurance services sector were about as likely to experience computer security incidents as businesses from most other sectors.

These findings challenge the perception that computer security incidents are becoming increasingly targeted. They may also provide one potential explanation for the somewhat unexpected finding that businesses from the financial and insurance services sector did not experience the highest proportion of computer security incidents.

Expenditure on computer security and number of computer security incidents experienced

The ABACUS data reveal a somewhat unclear relationship between expenditure on information technology security and the number of computer security incidents experienced.

In each of the lower expenditure brackets—less than \$1,000, \$1,000–9,999 and \$10,000–24,999—a substantial majority of businesses reported experiencing no computer security incidents. Eighty-three percent of businesses that spent less than \$1,000 on computer security reported no incidents, 73 percent of businesses spending between \$1,000 and \$9,999 reported no incidents and 71 percent of businesses spending between \$10,000 and \$24,999 reported no incidents.

This finding is somewhat surprising. A strong relationship between high levels of computer security *expenditure* and low levels of computer security *incidents* might have been expected. There are, however, a number of potential explanations for this anomaly:

- The majority of businesses reporting computer security expenditure in the lower brackets were small businesses. As discussed earlier in this report (see Table 8), small businesses reported

Table 31 Expenditure on information technology security by number of computer security incidents (percent)

	None	1–5	6–10	More than 10	Don't know	Weighted n
Less than \$1,000	83	11	1	1	5	2,075
\$1,000–9,999	73	17	2	2	6	770
\$10,000–24,999	71	18	3	5	3	94
\$25,000–74,999	46	32	4	8	10	25
\$75,000–99,999	100	0	0	0	0	1
\$100,000+	47	17	1	3	32	8

Note: n=2,974. Excludes 307 businesses with no information technology, 228 don't know responses and 492 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

lower information technology expenditure than medium businesses, and medium businesses reported lower expenditure than large businesses. The ABACUS data on information technology *security* expenditure also shows that small and medium businesses are more heavily concentrated in the lower expenditure brackets than large businesses. It is likely, therefore, that businesses that expended less on computer security may have experienced fewer computer security incidents due to their size, rather than the existence of a relationship between lower expenditure and fewer incidents.

- Small businesses may be less appealing targets and certainly have less information technology infrastructure than their large counterparts. Therefore, there is a reduced scope for the victimisation of small businesses and by extension, a reduced scope for the victimisation of businesses that expend only small amounts on computer security.
- These data may also suggest that businesses that expend only small amounts on computer security may be simply unaware that they have experienced computer security incidents. As discussed earlier in this report, some respondents may view computer security incidents as technical problems ('the computer crashed') rather than criminal ones.

Businesses' e-literacy and number of computer security incidents experienced

As indicated in Table 32, the majority of respondents to the ABACUS survey ranked their knowledge of and ability to use information technology as 'moderate'. This is a subjective assessment of respondents' knowledge and ability and as such, it is perhaps unsurprising that many respondents described their skills as 'moderate'.

A higher proportion of respondents who ranked their knowledge of and ability to use information technology as 'very high' reported experiencing more than 10 computer security incidents than six to 10 incidents. In turn, a higher proportion of those with 'very high' knowledge/ability experienced six to 10 incidents than one to five incidents and no incidents. Therefore, in contrast to what might be expected, respondents who rated their knowledge and ability of information technology as 'very high' also reported experiencing greater levels of computer security incidents. This may suggest that either there is no relationship between knowledge of and ability to use information technology and the prevention of computer security incidents, or that those with better knowledge/ability are simply more aware of the computer security incidents their business experiences.

Table 32 Respondents' knowledge of, and ability to use, information technology, by number of computer security incidents experienced (percent)

	None	1–5	6–10	More than 10	Don't know	Weighted n
Knowledge						
Very low	90	5	0	0	5	107
Low	84	7	1	1	8	422
Moderate	81	12	1	1	5	1,913
High	76	15	1	2	6	862
Very high	70	16	3	5	7	259
Total	80	12	1	1	6	3,563
Ability						
Very low	89	1	0	0	9	87
Low	86	6	1	0	8	350
Moderate	82	11	1	1	5	1,792
High	76	16	1	2	6	964
Very high	68	18	3	5	6	270
Total	79	12	1	1	6	3,462

Source: AIC, ABACUS 2008 [computer file, weighted data]

Nature of computer security incidents against Australian businesses



The ABACUS survey asked respondents to identify the types of computer security incidents their business had experienced during the 12-month period ending on 30 June 2007. Businesses were also asked about the proportion of incidents believed to have originated from within their organisation. Additionally, businesses were asked to provide information about the type of computer security incident they considered to be their business's most significant and the type of incident causing the greatest financial loss. This section presents these findings and compares findings from the ABACUS study with findings from previous research studies on computer security incidents against businesses.

Although previous surveys on computer security incidents against businesses have collected data on the types of incidents businesses experience, these data are not always directly comparable with the ABACUS data. The ABACUS findings, outlined below, indicate the proportion of businesses that experienced each type of incident *from the total number of businesses that experienced one or more computer security incidents* during the 2006–07 financial year. A number of existing surveys do not clarify whether they are reporting proportions of all businesses surveyed or all businesses experiencing an incident. In some, the number of businesses responding to questions about the type of incidents

experienced is higher than the number of businesses that reported experiencing an incident. As a result, the data from these surveys have not been used as a comparison in the following section. Surveys that have provided comparable data are included.

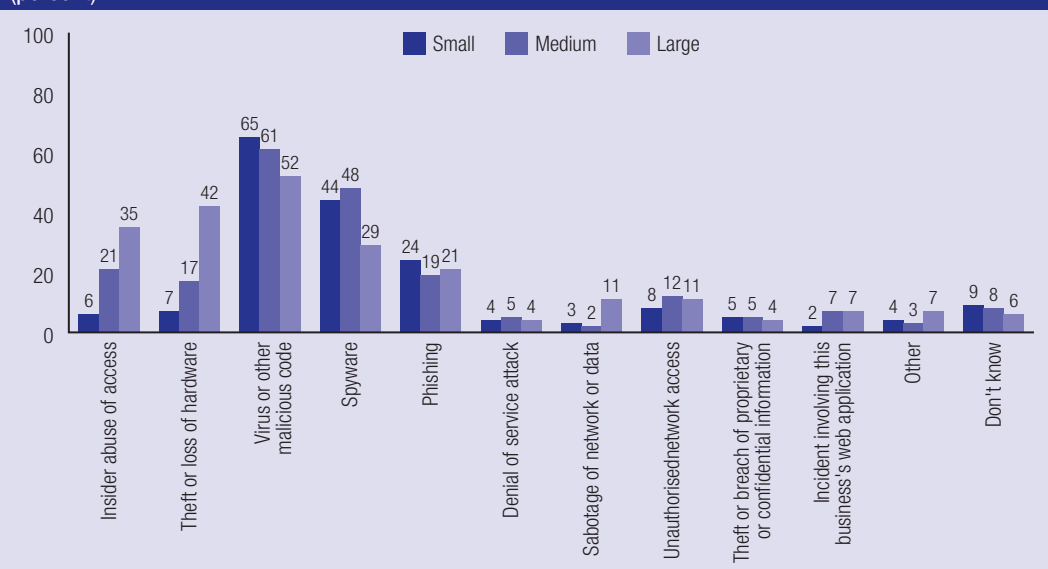
Types of computer security incidents experienced

As outlined in the previous section, 14 percent of ABACUS respondents reported experiencing one or more computer security incidents during the 12-month period ending 30 June 2007. Figure 23 shows the proportions of victimised small, medium and large businesses that experienced each type of computer security incident listed in the ABACUS survey. These computer security incidents were defined earlier in this report (see Glossary at Appendix 3).

As shown in Figure 23, of those businesses that experienced one or more computer security incidents, nine percent (6% of small, 21% of medium, 35% of large businesses) reported *insider abuse of access*.

Nine percent of victimised ABACUS businesses (7% of small, 17% of medium, 42% of large businesses) reported experiencing *theft or loss of hardware*.

Figure 23 Types of computer security incidents experienced by victimised businesses, by business size (percent)



Note: n=781. Excludes 307 businesses with no information technology, 2,881 businesses that experienced no computer security incidents and 31 missing answers (25 from small, 6 from medium, fewer than 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Sixty-four percent of ABACUS respondents that experienced one or more computer security incident (65% of small, 61% of medium, 52% of large businesses) reported experiencing a *virus or other malicious code*. Previous surveys have found diverse results in this regard. Rantala (2008: 3) found that 52 percent of respondents in the United States had experienced a virus. The survey by the Computer Emergency Response Team et al. (2007) of US businesses found that 74 percent had experienced viruses, worms or other malicious code. The findings of the ABACUS survey fall between these two estimates from existing surveys.

Forty-four percent of ABACUS respondents that had been victimised by one or more computer security incidents (44% of small, 48% of medium, 29% of large businesses) reported that their business experienced one or more *spyware* incidents in the 12-month period ending 30 June 2007. Research by the Computer Emergency Response Team et al. (2007) in the United States found a slightly higher proportion (52%) of businesses reported experiencing spyware.

Phishing attacks were experienced by 24 percent of victimised ABACUS respondents (24% of small,

19% of medium, 21% of large businesses).

Research by the Computer Emergency Response Team et al. (2007) found that 46 percent of businesses had experienced phishing incidents. In this survey, however, respondents were asked to indicate whether their business had been fraudulently represented as the sender of phishing emails. The ABACUS survey did not differentiate phishing attacks in which a business is itself fraudulently represented and phishing emails directed at businesses. It is therefore difficult to make meaningful comparisons between these two surveys. Nonetheless, these findings might be usefully considered alongside data from a recent report by the Anti-Phishing Working Group (2008). As a global organisation focused on eliminating phishing and pharming (see www.antiphishing.org), the Anti-Phishing Working Group collects and publishes data on phishing emails and websites reported by its member companies and recipients of phishing emails. The report estimates that the number of unique phishing sites reported in January 2008 was 20,305. Additionally, the report estimates that during January 2008, 131 brands (such as banks or credit card companies) were hijacked by phishers with the aim of convincing recipients to respond to phishing emails.

Four percent of victimised businesses in the ABACUS survey (4% of small, 5% of medium, 4% of large businesses) experienced a *denial of service* attack. In comparison, the Computer Emergency Response Team et al. (2007) found that 49 percent of respondents had experienced denial of service. The lower proportion of ABACUS respondents does not appear to be due to the higher proportion of small businesses in the ABACUS survey than other surveys on computer security incidents against businesses. Although denial of service incidents may be likely to have a greater impact when targeted towards large businesses, the ABACUS data show that similar proportions of businesses experienced denial of service attacks (see above).

Sabotage of network or data was experienced by three percent of ABACUS respondents (3% of small, 2% of medium, 11% of large businesses) that had been victimised by one or more computer security incident. Other surveys that have included a question on sabotage of network or data have produced varied results on this type of computer security incident. For example, Rantala (2008: 3) found that five percent of businesses had experienced 'vandalism or sabotage'. These results closely reflect the ABACUS findings. The Computer Emergency Response Team et al. (2007) found that 30 percent of respondents reported experiencing sabotage. In this survey, sabotage was defined as *deliberate disruption, deletion or destruction of information, systems or networks*. As noted previously, research by the Computer Emergency Response Team et al. (2007) surveyed computer security executives and law enforcement officials on experiences of computer security incidents. This approach, in contrast with surveying a representative sample of business sizes and industry sectors, is likely to yield results that indicate higher levels of computer security incidents. In comparison with ABACUS respondents, perhaps especially those from small businesses, respondents from information technology security backgrounds are potentially more likely to have increased levels of awareness and concern in relation to computer security incidents experienced. Additionally, experts in computer security may have more to gain from reporting high levels of computer security incidents. These factors may help explain the finding of the Computer Emergency Response Team et al. (2007) of a much higher proportion of businesses

experiencing sabotage than that found in other research.

Only nine percent of victimised businesses in the ABACUS survey (8% of small, 12% of medium, 11% of large businesses) reported experiencing *unauthorised network access*. In contrast, the Computer Emergency Response Team et al. (2007) found that 55 percent of respondents had experienced unauthorised access to or use of information, systems or networks. This finding may again be partly a result of the focus of the Computer Emergency Response Team et al. (2007) on computer security and law enforcement officials (see above). Additionally, the description by the Computer Emergency Response Team et al. of the type of incident — 'unauthorized access to/use of information, systems or networks' — is perhaps slightly broader than the ABACUS survey's 'unauthorised network access'. This may have increased affirmative responses to this category of computer security incident. Although a strong relationship between outsourced computer security measures and unauthorised network access may be expected, the ABACUS data suggest that only a slightly higher percentage (13%) of victimised businesses that had outsourced one or more security functions had experienced this type of attack than victimised businesses that had not outsourced any security functions (8%).

Five percent of ABACUS respondents (5% of small and medium businesses, 4% of large businesses) that had experienced one or more computer security incidents reported *theft or breach of proprietary or confidential information*. The Computer Emergency Response Team et al. (2007) again found a much higher proportion of businesses (40%) had experienced theft of proprietary information, including customer records and financial records. The lower proportion of ABACUS respondents that reported experiencing this type of computer security incident does not appear to reflect the nature of the survey's sample, which in contrast to existing surveys, included a representative proportion of small businesses. Similar proportions of small (5%), medium (5%) and large (4%) victimised businesses in the ABACUS survey reported experiencing theft or breach of proprietary or confidential information. The considerably higher proportion of businesses found by the Computer Emergency Response Team et al. to be reporting this type of computer security

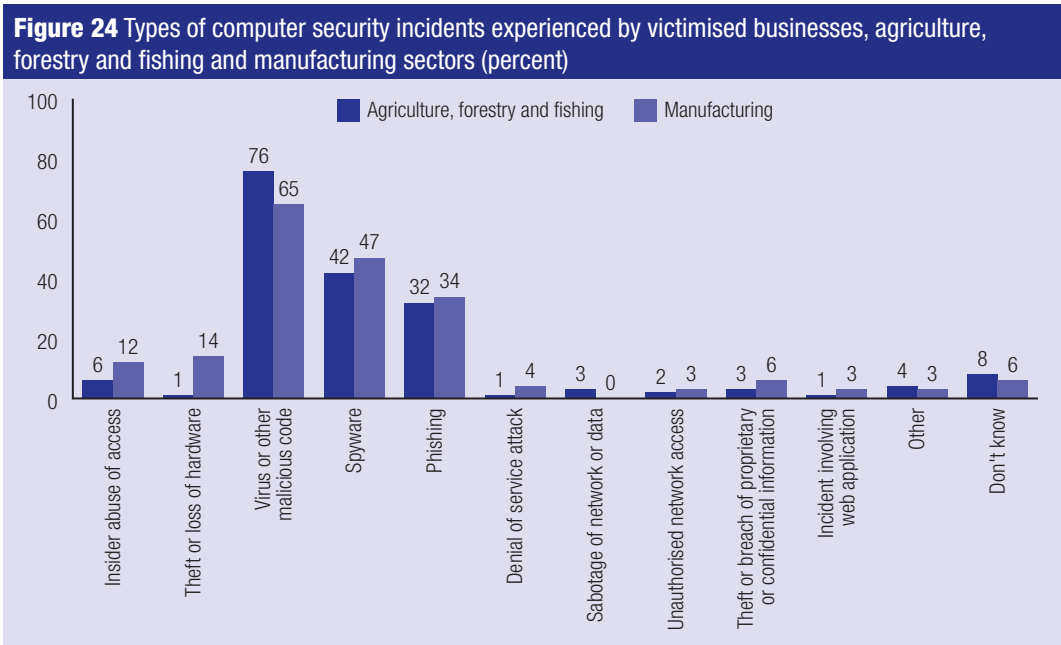
incident may again be due to the selection of respondents (see above). Additionally, in a number of instances, the Computer Emergency Response Team et al. (2007) used more detailed descriptions of computer security incidents than other surveys on computer security incidents against businesses have done. For example, this survey asked respondents whether they had experienced ‘theft of other (proprietary) info including customer records, financial records etc’. This more detailed description, in contrast with the ABACUS survey’s ‘theft or breach of proprietary or confidential information’, may have contributed towards the higher proportions of businesses reporting computer security incidents in the survey by the Computer Emergency Response Team et al. This was the case across a number of computer security incidents, including those asking about viruses, phishing, sabotage and unauthorised network access.

Three percent of victimised ABACUS respondents (2% of small, 7% of medium, 7% of large businesses) reported experiencing an incident involving their business’s *web application*. There are no comparable data on this type of computer security incidents from previous surveys.

Types of computer security incidents experienced by industry sectors

The ABACUS data show that victimised businesses from each industry sector experienced similar levels of each type of computer security incident. Viruses or other malicious code was the type of computer security incident experienced by the highest proportion of each industry sector. Figure 24 shows the pattern of incidents for two industry sectors: agriculture, forestry and fishing and manufacturing. This pattern of victimisation is similar across all industry sectors.

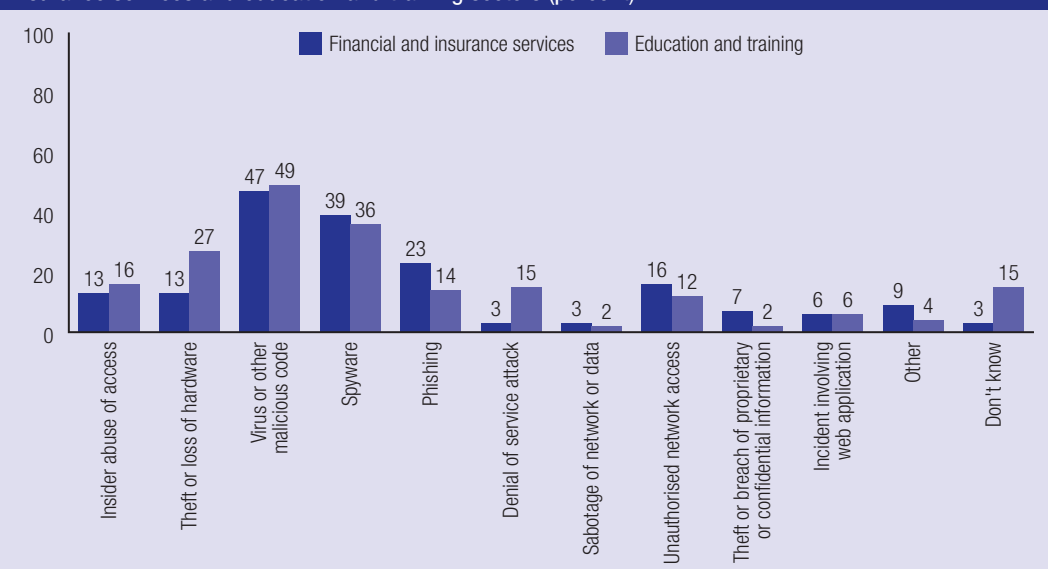
The financial and insurance services and education and training services sectors reported the least variation in relation to the types of computer security incidents experienced. As Figure 25 shows, proportions of victimised businesses from the financial and insurance services sector vary from three percent reporting denial of service attacks and sabotage of network or data to 47 percent reporting viruses or other malicious code. Similarly, in the education and training service sector, proportions



Note: n=781. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 31 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

Figure 25 Types of computer security incidents experienced by victimised businesses, financial and insurance services and education and training sectors (percent)



Note: n=781. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 31 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

of victimised businesses ranged from two percent reporting sabotage of network or data and theft or breach of proprietary or confidential information to 49 percent reporting viruses or other malicious code. For other sectors, this variation was more pronounced (see Figure 24). Overall, however, the pattern of victimisation across industry sectors was very similar.

Computer security incidents originating from within businesses

The existing literature and research on computer security incidents against businesses suggests that businesses are concerned about the threat of incidents originating from employees of the organisation (Darrow 2008). Deloitte Touche Tohmatsu (2007: 25) found that approximately one-quarter of respondents to their survey predicted that 'internal financial fraud involving information systems' would be a major threat within the 12 months following the survey and more than

half of respondents predicted this would be a moderate threat. 'Employee misconduct' was similarly rated as a major threat by around one-quarter of respondents and a moderate threat by over half of respondents (Deloitte Touche Tohmatsu 2007: 25). Ho's (2006: 13) research into businesses' attitudes in relation to computer security incidents found that 75 percent of Australian respondents considered threats to corporate security to be coming from within their organisation (see also Webroot Software 2008b). Attacks by insiders are thus 'widely recognised as an issue of utmost importance' (Choo, Smith & McCusker 2007a: 53). As Walton (cited in Choo, Smith & McCusker 2007a: 51) argues, while the *motivation* for perpetrating computer security incidents against businesses may be greater for outsiders, the *ability* to do so is greater for insiders.

The ABACUS questionnaire asked respondents that indicated they had experienced computer security incidents within the 12 month period ending 30 June 2007 to identify what percentage of incidents originated from a person or persons within their business. Sixty-one percent of respondents that used information technology and experienced

one or more computer security incidents reported that no computer security incidents originated from within their business.

Table 33 Computer security incidents originating from within, by business size (percent)				
	Small	Medium	Large	Weighted n
0	66	35	39	461
1–9	1	8	6	15
10–24	1	<1	6	6
25–49	<1	<1	4	2
50–74	1	5	2	12
75–100	4	16	22	47
Don't know	27	35	20	212
Total	100	100	100	756

Note: Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 56 missing answers (48 from small, 8 from medium, fewer than 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

As shown in Table 33, considerable proportions of small (66%), medium (35%) and large (39%) victimised businesses reported experiencing no computer security incidents originating from within their organisation. Importantly, however, large proportions of respondents from small (27%), medium (35%) and large (20%) businesses did not know what proportion of computer security incidents were originating from within their businesses.

Considerable proportions of medium and large businesses also reported that 75–100 percent of computer security incidents experienced had originated from within their organisation. In general, higher proportions of large businesses appear to have experienced computer security incidents originating from employees.

There are a number of potential explanations for this finding:

- Large businesses in the ABACUS survey had, by definition, more employees than small or medium businesses. As outlined above, small businesses in the ABACUS study were defined as those with 0–19 employees, medium businesses as those with 20–199 employees and large businesses as those with 200 or more employees. The greater number of employees in large businesses may result in these businesses having more autonomous and less closely monitored staff.

- Large businesses are potentially more likely to have staff in more specialised and dedicated information technology positions, who may therefore have more detailed knowledge of, and skills in, information technology. Such staff may therefore be better able to perpetrate computer security incidents against their employers than staff at smaller organisations.
- It is also possible that staff at larger companies experience greater alienation from company objectives and/or less loyalty towards their employers, and are therefore more likely to perpetrate computer security incidents against them.
- Finally, large businesses may present a more appealing target than small or medium businesses. Employees may be familiar with the financial status of the company they are employed by, and may be aware of the likelihood of their being discovered should they perpetrate a computer security incident.

Importantly, this finding may be used to inform large businesses' use of computer security policies. As discussed above (see Figure 10), although large proportions of large businesses reported using an information technology acceptable use policy (78%) and account or password management policies (70%), these proportions are somewhat lower than might have been expected and are certainly lower than the proportions of businesses that reported using these policies in other surveys. Moreover, only around half of large businesses reported monitoring staff internet connections (52%), using employee education and awareness programs (49%) and user access management policies (53%). Less than one-quarter of businesses reported using background checks (24%) and policies requiring mandatory reporting of misuse or abuse of computer equipment (22%). Large businesses may use this finding to increase their use of computer security policies aimed at curbing incidents originating from within organisations.

These findings depart somewhat from the findings of existing surveys of computer security incidents against businesses. As shown in Figure 26, the ABACUS survey found that a much larger proportion of businesses had experienced no computer security incidents perpetrated by insiders than

that found by other surveys on computer security incidents against businesses. There are a number of potential explanations for this.

The high proportion of small businesses in the ABACUS survey's representative sample is likely to have impacted on this finding. As discussed above, small businesses have fewer employees with less specialised skills than larger businesses. Staff in small businesses may be more closely monitored and less technologically capable than their counterparts in large businesses. Small businesses usually have lower annual turnovers than large businesses and may therefore present less appealing targets than larger businesses. Small business employees are therefore less likely to have the ability, opportunity or desire to perpetrate computer security incidents against their employer.

The type of question asked of ABACUS respondents may have contributed towards this much higher finding. ABACUS respondents were asked to indicate what percentage of all computer security incidents experienced by their business had originated from within the organisation. This type of question is potentially likely to dichotomise responses, as respondents may be aware that 'most' or 'none' of their security incidents were perpetrated by insiders, rather than having knowledge of a specific percentage.

Importantly, 28 percent of respondents reported that they did not know what proportion of their business's computer security incidents had originated from within their organisation. These responses have been included in the calculation above (see Figure 26). Had they been excluded, the proportion of businesses experiencing no computer security incidents from within their organisation would be higher again, at 85 percent.

Results from Rantala's (2008: 7) survey suggest that certain types of computer security incidents may be more likely to be perpetrated by insiders than other types of incidents. For example, Rantala found that while the majority of victims of cyber theft suspected the perpetrator was an insider, the opposite was true in relation to other types of computer security incidents.

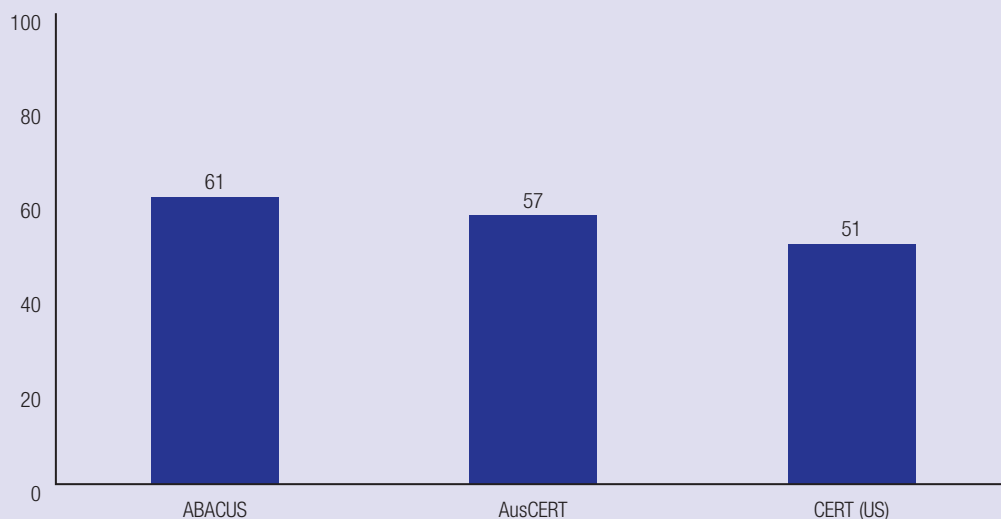
Businesses from the transport, postal and warehousing sector reported the highest level of computer security incidents originating from within their business (34%; see Figure 27). The lowest level of computer security incidents originating from within came from the administrative and support services sector (6%). Figure 27 shows the proportions of businesses from each industry sector that experienced computer security incidents originating from within their organisation.

Computer security incidents causing greatest financial loss

Respondents whose businesses had experienced one or more computer security incidents were asked to identify the type of incident that caused the greatest financial loss to their business. Financial loss was defined in the ABACUS survey as including *all costs associated with the incident/s. These may include aspects such as the direct financial cost of the incident, staff costs in repairing the damage caused, loss of revenue due to the incident or any other cost that was a direct result of the incident.* Respondents were instructed that costs relating to computer security measures implemented before or after the incident were to be excluded.

The highest proportion of small (39%) and medium (26%) victimised businesses reported viruses and other malicious code as the computer security incident causing the greatest financial loss. For large victimised businesses, theft or loss of hardware (29%) was reported as causing the greatest financial loss, followed by viruses and other malicious code (26%). Medium businesses listed theft or loss of hardware and insider abuse of access (both 12%) after viruses and other malicious code. As shown in Table 34, small businesses reported spyware (11%) as the computer security incident causing greatest financial loss after viruses and malicious code. For small businesses, spyware ranked more highly than for medium (9%) or large (<1%) businesses.

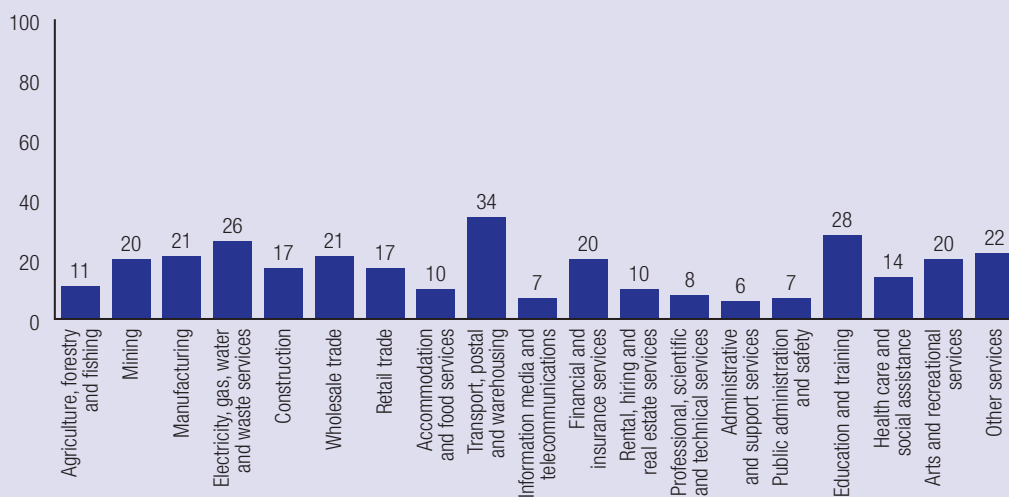
Figure 26 Businesses that experienced no computer security incidents perpetrated by insiders, comparison with other surveys (percent)



Note: ABACUS n=756. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 56 missing answers. AusCERT n=86. CERT n=unknown

Source: AIC, ABACUS 2008 [computer file, weighted data]

Figure 27 Businesses experiencing one or more computer security incidents originating from within the organisation, by sector (percent)



Note: n=544. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents, 212 don't know responses and 56 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

Most significant computer security incidents experienced by businesses

Respondents whose businesses had experienced one or more computer security incidents were also asked to identify the type of the *most significant* incident that had affected their business in the 12-month period ending on 30 June 2007.

Respondents were instructed to regard their most significant computer security incident as *the one that your business regards as causing the greatest negative effect or loss. Such incidents may include ones that caused the greatest financial loss, caused damage to your business's reputation and/or other negative effects.*

Viruses and other malicious code again rank highly as victimised businesses' most significant incident, with considerable proportions of small (57%), medium (39%) and large (26%) businesses identifying this type of computer security incident as their most significant. As indicated in Table 35, 14 percent of small victimised businesses listed spyware as their most significant computer security incident. Again, this represents a higher proportion of small business than medium (10%) or large (9%) victimised businesses. After viruses and other malicious code, medium businesses were most likely to report insider abuse of access as their most significant computer security incident, with 15 percent of medium businesses reporting this type of incident. The highest proportion of large businesses (28%) identified theft or loss of hardware as their most significant computer security incident, followed by viruses and other malicious code, which 16 percent of large businesses listed as their most significant incident.

Businesses ranked their most significant computer security incident and the type of incident causing the greatest financial loss to their business in similar patterns. This suggests that businesses regard significant computer security incidents as those causing financial loss (compare Tables 34 and 35).

Table 34 Computer security incident causing greatest financial loss, by business size (percent)

	Small	Medium	Large	Weighted n
Insider abuse of access	3	12	17	37
Theft or loss of hardware	5	12	29	47
Virus or other malicious code	39	26	26	276
Spyware	11	9	<1	76
Phishing	3	5	0	22
Denial of service attack	1	2	1	10
Sabotage of network or data	1	1	5	10
Unauthorised network access	2	7	1	22
Theft or breach of proprietary or confidential information	3	3	0	25
Incident involving the business's web application	1	<1	<1	7
Spam	<1	<1	0	1
Other	2	<1	7	12
Don't know	23	18	12	162
No incidents caused financial loss	6	3	<1	39
Total	100	100	100	744

Note: Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 68 missing answers (63 from small, 5 from medium businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 35 Most significant computer security incident, by business size (percent)

	Small	Medium	Large	Weighted n
Insider abuse of access	3	14	14	37
Theft or loss of hardware	4	10	24	39
Virus or other malicious code	48	35	23	349
Spyware	12	9	8	85
Phishing	5	6	0	38
Denial of service attack	2	2	1	12
Sabotage of network or data	1	0	8	7
Unauthorised network access	4	6	5	32
Theft or breach of proprietary or confidential information	3	1	1	24
Incident involving the business's web application	1	3	3	11
Spam	<1	0	0	2
Other	2	<1	0	10
Don't know	15	13	14	111
Total	100	100	100	756

Note: Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 56 missing answers (48 from small, 8 from medium, fewer than 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Effects of computer security incidents against Australian businesses

Respondents to the ABACUS survey were asked to identify the types of effects that their business had suffered as a result of computer security incidents. These effects, both financial and non-financial, are outlined below.

Effects of computer security incidents against businesses

Respondents were asked to identify the effects that their business's most significant computer security incident had caused. Businesses were asked about:

- *corruption of hardware or software*: damage to computer hardware or software that renders it non-operational
- *corruption of loss of data*: damage to or interference with data that renders it non-operational
- *unavailability of service*: making the operations of a business, either in part or in whole, unavailable
- *website defacement*: damage caused to a public website that limits or prevents its intended use
- *theft or loss of hardware*: hardware, such as laptops, Personal Digital Assistants or other devices are lost or stolen and not recovered. This does not include hardware that is damaged or destroyed
- *theft of business, confidential or proprietary information*: unauthorised access to and/or use, viewing, duplication, distribution or theft of information relating to a business's product or activities, such as financial information
- *non-critical operational losses*: disruption to a business that did not cause suspension or severe damage to the business's operations
- *non-critical financial losses*: loss of money or value to a business that did not cause a severe negative alteration to the business's financial state
- *harm to reputation*: reduction in confidence in or increase in negative association with a business
- *critical operational losses*: disruption to a business that causes suspension or severe damage to a business
- *critical financial losses*: loss of money or value to a business that causes severe negative alteration to the business
- *loss of life*: the death of a person who was, or was not, an employee of a business.

A majority of businesses overall (77%) reported experiencing some type of negative impact following their most significant computer security incident (75% of small, 88% of medium, 95% of large businesses). As indicated in Table 36, the type of impact experienced varies according to business size. Small (42%) and medium (35%) businesses were most likely to experience corruption of hardware or software. Large businesses were most likely to experience theft or loss of hardware (40%), followed by unavailability of service (39%). Importantly, nine percent of businesses overall (9% of small, 12% of medium, 14% of large businesses) did not know whether their business had experienced any of the results listed in the ABACUS survey following its most significant computer security incident (see Table 36).

Table 36 Impacts experienced as a result of most significant computer security incident, by business size (percent)

	Small	Medium	Large	Weighted n
Corruption of hardware or software	42	35	31	278
Corruption of loss of data	31	30	31	213
Unavailability of service	38	33	39	259
Website defacement	2	<1	6	14
Theft or loss of hardware	4	9	40	38
Theft of business, confidential or proprietary information	5	5	17	35
Non-critical operational losses	24	27	31	171
Non-critical financial losses	12	14	12	85
Harm to reputation	4	4	8	30
Critical operational losses	4	3	14	26
Critical financial losses	5	2	3	29
Loss of life	0	0	0	0
Other	1	<1	6	5

Note: n=687. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents, 72 don't know responses and 54 missing answers (49 from small, 5 from medium, fewer than 1 from large businesses)

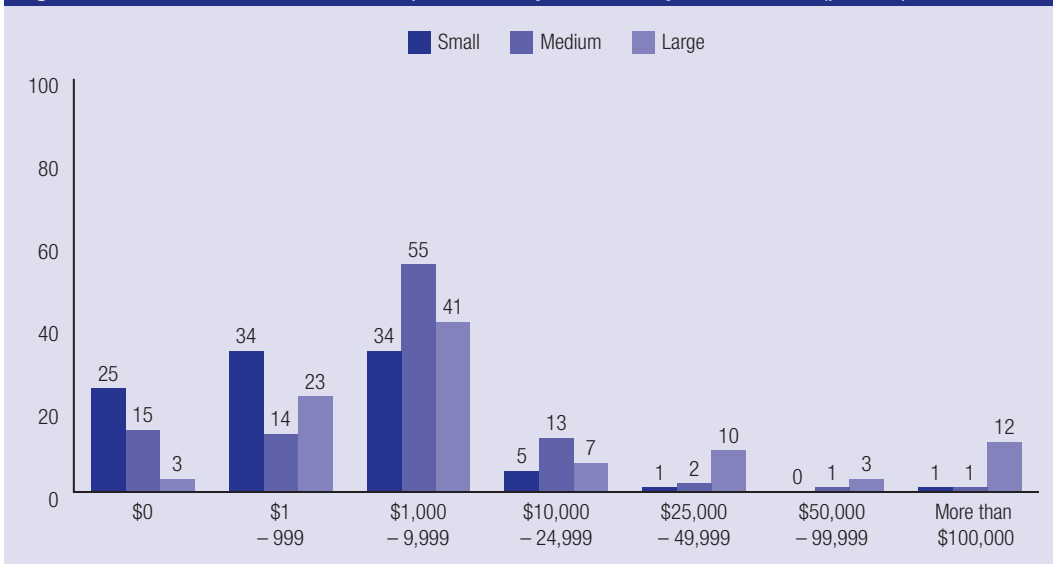
Source: AIC, ABACUS 2008 [computer file, weighted data]

Financial losses resulting from computer security incidents

Respondents were asked to estimate the total financial losses from all computer security incidents to their business during the 2006–07 financial year. Financial losses were defined as *all costs associated with the incident/s. These may include aspects such as the direct financial cost of the incident, staff costs in repairing the damage caused, loss of revenue due to the incident or any other cost that was a direct result of the incident.* Computer security measures implemented either before or after an incident occurred were excluded.

The highest proportion of small (33%), medium (40%) and large (34%) businesses that had experienced a computer security incident during the 12-month period ending on 30 June 2007 reported that the total financial cost of all security incidents during the period was between \$1,000 and \$9,999. As shown in Figure 28, the next highest proportion for small businesses was the 30 percent that reported a total financial cost of between \$1 and \$999. Fourteen percent of medium businesses reported that there had been no financial losses as a result of computer security incidents, followed by 10 percent who reported losses of between \$1 and \$999. Large businesses reported higher losses overall, with 17 percent experiencing losses of between \$10,000 and \$24,999, 11 percent between \$1 and \$999 and nine percent in excess of \$100,000.

The mean loss from computer security incidents overall was \$699. For small businesses the mean loss was \$360, for medium businesses the mean loss was \$2,757 and for large businesses the mean loss was \$17,578. These figures represent *all businesses*, including those that did not have any information technology and/or did not experience any computer security incidents in the 12-month period ending 30 June 2007. The mean loss resulting from computer security incidents of businesses that experienced computer security incidents during the period was \$4,469. For small businesses the mean loss was \$2,431, for medium businesses the mean loss was \$12,405 and for large businesses the mean loss was \$49,246. Table 37 shows the financial losses from computer security incidents during the 2006–07 financial year.

Figure 28 Total financial cost of all computer security incidents, by business size (percent)

Note: n=673. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 139 missing answers (126 from small, 12 from medium, 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 37 Estimated financial losses from all computer security incidents, by business size (\$)

	Median ^a	Mean	Min	Max
Median, mean and range of losses from computer security incidents against businesses ^b				
Small	0	360	0	100,000
Medium	0	2,757	0	500,000
Large	0	17,578	0	600,000
Businesses overall	0	699	0	600,000
Median, mean and range of losses from computer security incidents against businesses experiencing computer security incidents ^c				
Small	500	2,431	0	100,000
Medium	2,000	12,405	0	500,000
Large	5,000	49,246	0	600,000
Businesses overall	600	4,469	0	600,000

a: Medians are estimates, due to the use of weighted data

b: n=3,779. Excludes 221 missing answers

c: n=591. Excludes 307 businesses with no information technology, 2,881 that did not experience any computer security incidents and 221 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

The sample of Australian businesses surveyed in the ABACUS study allows an estimate of the total losses from all computer security incidents against

Australian businesses to be made. As discussed earlier in this report, the ABACUS sample was large enough to provide representative data for all businesses and was weighted to accurately reflect the composition of the Australian business population. Data collected during the ABACUS study can therefore be multiplied out to produce a weighted estimate of the total financial losses resulting from computer security incidents against all Australian businesses.

Providing an estimate of the total losses stemming from computer security incidents is a challenging task. Business respondents to the ABACUS survey were asked to provide their *best estimate* of dollar losses resulting from all computer security incidents during the 2006–07 financial year. The ABACUS survey did not collect exact figures of losses in order to minimise non-response to this question.

Additionally, there were a high number of missing data for this question, with 221 missing answers. As discussed earlier, a high level of non-response is common for survey questions that ask respondents for financial information. These missing data are nonetheless important to consider in estimations of losses resulting from computer security incidents against the total population of Australian businesses.

As indicated in Table 38, there are a number of methods for calculating this estimate based on the ABACUS data, which produce estimates ranging from \$595m to \$649m.

The first method substitutes a \$0 value for businesses that did not provide an estimate of their financial losses from computer security incidents. This method relies on the assumption that respondents that did not experience any losses from computer security incidents believed that leaving the question unanswered was the same as providing an answer of \$0. Using this approach, a \$0 value is substituted as the total loss from all computer security incidents for all non-responding businesses. This method of calculating an estimate of Australian businesses' losses produces a conservative estimate of \$595m (see Table 38). This same estimate is obtained when calculating total losses from computer security incidents across all Australian businesses, *excluding* those that did not provide an answer to this question.

The second method substitutes the *mean* losses from computer security incidents of businesses that provided an answer for those that did not. The mean of \$699 is substituted for all businesses that did not provide an estimate of their financial losses from computer security incidents. This mean is based only on the estimates given by respondents to the question. That is, it excludes all non-respondents. This method produces an estimate of \$644m (see Table 38).

The third method substitutes the median losses from computer security incidents against businesses for businesses that did not provide an answer. As the median losses resulting from computer security incidents against businesses is \$0, the same estimate is produced as for method 1 (see above) of \$595m. It is important to note that due to the skewed nature of the ABACUS data on this variable, the *median* is a more robust measure of central tendency than the *mean*.

The final method used to estimate the total financial losses stemming from computer security incidents against all Australian businesses was to substitute a predicted value for non-respondents based on industry sector and business size. This method involved using a binomial regression analysis to predict non-respondents' financial losses based on their industry sector and business size. Rather than

substituting the *same* measure of central tendency (mean or median) for each non-responding business, this approach substituted a *unique* estimate for each non-responding business. These estimates used the businesses' industry sector and number of employees to predict an approximate value for their losses from computer security incidents. This method, which takes into account the characteristics of non-respondents and the likely effects of these characteristics on their financial losses, produces the most robust estimate of the total losses of all Australian businesses. The method produces an estimate of \$649m.

Table 38 Estimated financial losses from all computer security incidents across Australian businesses (\$)				
	Estimate 1	Estimate 2	Estimate 3	Estimate 4
Small	276m	317m	276m	293m
Medium	218m	226m	218m	242m
Large	101m	101m	101m	114m
Businesses overall	595m	644m	595m	649m

Source: AIC, ABACUS 2008 [computer file, weighted data]

Businesses from the manufacturing sector reported the highest mean losses from computer security incidents (\$2,354), followed by the retail sector (\$1,353). Lowest mean losses were experienced by the agriculture, forestry and fishing sector (\$183), followed by the arts and recreational services and other services sector (both \$261). The highest total losses from computer security incidents were reported by the retail (\$600,000) and manufacturing (\$500,000) sectors (see Table 39).

Table 40 shows the median, mean, minimum and maximum financial losses for those businesses that reported experiencing one or more computer security incidents, focusing only on those businesses that experienced incidents results in considerably higher median and mean dollar losses. The manufacturing sector still reported the highest mean losses from computer security incidents (\$13,295), followed by the retail sector (\$9,870). Lowest mean losses were experienced by the agriculture, forestry and fishing services sector (\$1,155), followed by the public administration and safety sector (\$2,010; see Table 40).

Table 39 Estimated financial losses from all computer security incidents, by sector (\$)

	Median ^a	Mean	Minimum	Maximum
Agriculture, forestry and fishing	0	183	0	15,000
Mining	0	434	0	50,000
Manufacturing	0	2,354	0	500,000
Electricity, gas, water and waste services	0	318	0	15,000
Construction	0	267	0	30,000
Wholesale trade	0	889	0	40,000
Retail trade	0	1,353	0	600,000
Accommodation and food services	0	401	0	35,000
Transport, postal and warehousing	0	632	0	250,000
Information media and telecommunications	0	853	0	80,000
Financial and insurance services	0	715	0	100,000
Rental, hiring and real estate services	0	856	0	50,000
Professional, scientific and technical services	0	365	0	20,000
Administrative and support services	0	1,170	0	110,000
Public administration and safety	0	443	0	20,000
Education and training	0	619	0	95,000
Health care and social assistance	0	851	0	100,000
Arts and recreational services	0	261	0	15,000
Other services	0	261	0	20,000
Total	0	699	0	600,000

a: Medians are estimates, due to the use of weighted data

Note: n=3,779. Excludes 221 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 40 Estimated financial losses from all computer security incidents across businesses experiencing computer security incidents, by sector (\$)

	Median ^a	Mean	Minimum	Maximum
Agriculture, forestry and fishing	300	1,155	0	15,000
Mining	1,000	3,721	0	50,000
Manufacturing	1,000	13,295	0	500,000
Electricity, gas, water and waste services	400	2,676	0	15,000
Construction	500	2,063	0	30,000
Wholesale trade	1,000	5,175	0	40,000
Retail trade	1,000	9,870	0	600,000
Accommodation and food services	500	2,924	0	35,000
Transport, postal and warehousing	1,300	4,636	0	250,000
Information media and telecommunications	1,000	4,262	0	80,000
Financial and insurance services	1,000	4,837	0	100,000
Rental, hiring and real estate services	500	3,801	0	50,000
Professional, scientific and technical services	1,000	1,863	0	20,000
Administrative and support services	500	5,790	0	110,000
Public administration and safety	500	2,010	50	20,000
Education and training	1,000	2,843	0	95,000
Health care and social assistance	400	5,468	0	100,000
Arts and recreational services	500	2,073	0	15,000
Other services	450	2,533	0	20,000
Total	600	4,469	0	600,000

a: Medians are estimates, due to the use of weighted data

Note: n=591. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents, 80 don't know responses and 139 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]

The four methods used above to estimate the total financial losses stemming from computer security incidents for all Australian businesses for the 2006–07 period were also used to calculate estimates of losses by industry sector. Table 41 shows the four estimates calculated for each industry sector. As discussed above, the fourth estimate, which uses a predicted value for each non-responding business, is the most robust (see Table 41).

As indicated in Table 42, there does not appear to be a strong relationship between respondents' knowledge of and ability to use information technology and the cost of computer security incidents experienced by businesses. Although we might expect that those with higher levels of information technology skills and knowledge would report lower overall losses from computer security incidents, this does not appear to be the case.

There are a number of possible reasons for this somewhat unexpected finding:

- Respondents were asked to assess their own knowledge of and ability to use information technology. The ABACUS data on businesses'

information technology skills and knowledge is therefore a subjective assessment only. It is possible, therefore, that a relationship between ability to use information technology and decreased losses from computer security incidents may have been obscured by respondents' subjective assessment of their computer ability.

- It is also possible that there is no direct relationship between the computer skills of respondents and the level of financial losses experienced as a result of computer security incidents. It is likely that those with low level computer skills rely less on information technology within their businesses. Businesses with less information technology are, in turn, probably less likely to experience computer security incidents.
- Respondents with limited information technology knowledge may also simply be unaware of computer security incidents that have occurred. This could also help explain the apparent lack of relationship between reported computer skills and the number of computer security incidents experienced by businesses.

Table 41 Estimated financial losses from computer security incidents across all Australian businesses, by sector (\$)

	Estimate 1	Estimate 2	Estimate 3	Estimate 4
Agriculture, forestry and fishing	12.0m	14.5m	12.0m	12.5m
Mining	1.3m	1.7m	1.3m	1.7m
Manufacturing	121m	125m	121m	127m
Electricity, gas, water and waste services	0.8m	0.9m	0.8m	0.8m
Construction	32.3m	40.5m	32.3m	33.9m
Wholesale trade	36.8m	38.6m	36.8m	39.7m
Retail trade	109m	114m	109m	115m
Accommodation and food services	22.1m	24.5m	22.1m	23.2m
Transport, postal and warehousing	26.4m	27.9m	26.4m	29.4m
Information media and telecommunications	6.3m	6.9m	6.3m	6.7m
Financial and insurance services	48.9m	51.5m	48.9m	54.8m
Rental, hiring and real estate services	26.5m	29.7m	26.5m	30.8m
Professional, scientific and technical services	39.5m	44.8m	39.5m	45.3m
Administrative and support services	40.1m	44.1m	40.1m	46.3m
Public administration and safety	1.6m	2.0m	1.6m	2.0m
Education and training	8.1m	9.3m	8.1m	9.1m
Health care and social assistance	43.6m	45.9m	43.6m	51.4m
Arts and recreational services	3.2m	4.0m	3.2m	3.5m
Other services	15.3m	18.7m	15.3m	16.1m
Total	595m	644m	595m	649m

Source: AIC, ABACUS 2008 [computer file, weighted data]

Table 42 Respondents' knowledge of, and ability to use, information technology, by total cost of computer security incidents (percent)

	\$0	\$1–999	\$1,000– 9,999	\$10,000– 24,999	\$25,000– 49,999	\$50,000– 99,999	\$100,000+	Don't know	Weighted n
Knowledge									
Very low	2	1	1	0	0	0	0	<1	8
Low	10	11	7	5	0	0	0	11	56
Moderate	50	57	46	51	43	41	36	45	324
High	28	24	34	31	41	7	49	33	196
Very high	11	6	13	13	17	52	15	11	69
Total	100	100	100	100	100	100	100	100	653 ^a
Ability									
Very low	2	1	0	0	0	0	0	<1	4
Low	7	10	4	2	0	0	0	10	43
Moderate	46	51	44	38	48	41	0	40	291
High	32	27	39	37	49	7	82	40	221
Very high	12	11	14	22	3	52	18	10	83
Total	100	100	100	100	100	100	100	100	642 ^b

a: Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 159 missing answers

b: Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 170 missing answers

Source: AIC, ABACUS 2008 [computer file, weighted data]



Responding to computer security incidents against Australian businesses

ABACUS respondents were asked a number of questions about how they responded to computer security incidents against their business. Businesses' reporting behaviours, and satisfaction with the outcomes of these behaviours, are discussed in this section. Where appropriate, these findings have been compared with those of previous surveys on computer security incidents against businesses.

Reporting computer security incidents against Australian businesses

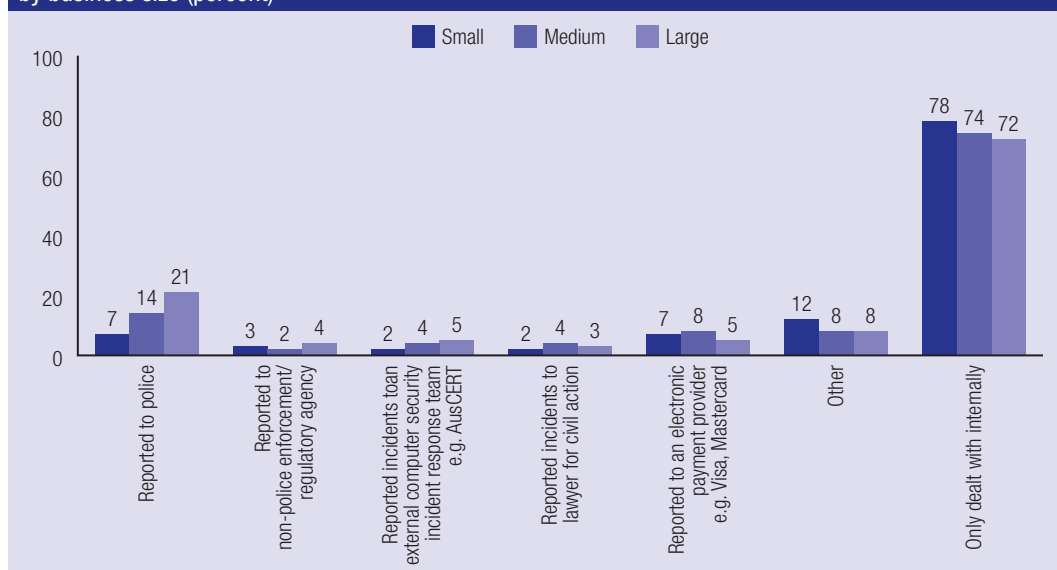
The literature on computer security incidents frequently asserts that those affected by computer security incidents are unlikely to report them to a third party such as the police or other law enforcement agency (e.g. see Hughes & DeLone 2007).

The ABACUS survey asked respondents to identify what action they took following the *most significant* computer security incident that affected their business during the 12-month period ending 30 June 2007 (see Figure 29). Respondents were able to select multiple responses for this question on reporting behaviours following computer security incidents.

Seventy-seven percent of businesses (77% of small, 74% of medium, 72% of large businesses) that experienced one or more computer security incident dealt with the most significant computer security incident internally and did not report it to any external agency. Eight percent of victimised businesses (7% of small, 14% of medium, 21% of large businesses) reported their most significant incident to the police, seven percent (7% of small, 8% of medium, 5% of large businesses) to an electronic payment provider such as Visa or Mastercard, three percent (3% of small, 2% of medium, 4% of large businesses) to a non-police enforcement or regulatory agency, two percent (2% of small, 4% of medium, 3% of large businesses) to a lawyer and two percent (2% of small, 4% of medium, 5% of large businesses) to an external computer security incident response team such as AusCERT. This is consistent with a majority of research on cybercrime and white collar crime more generally, which suggests that businesses rarely report incidents to law enforcement agencies, but prefer to deal with incidents internally.

These findings suggest that business size is associated with businesses' decisions to report computer security incidents, with large businesses most likely to do so. There are a number of potential explanations for the higher proportion of large businesses reporting computer security incidents to police.

Figure 29 Action taken by victimised businesses following most significant computer security incident, by business size (percent)



Note: n=766. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 46 missing answers (40 from small, 6 from medium, fewer than 1 from large businesses)

Source: AIC, ABACUS 2008 [computer file, weighted data]

Large businesses may suffer a greater financial impact than medium or small businesses, and this may in turn influence businesses' decisions to report incidents to police. The ABACUS data indicate that large businesses do in fact suffer greater financial losses than medium or small businesses, with large victimised businesses more likely to report losses of \$100,000 or more for their total computer security incident costs. Large victimised businesses (6%) were also far less likely than medium (14%) or small victimised businesses (20%) to report no financial costs from computer security incidents during the 12-month period ending 30 June 2007.

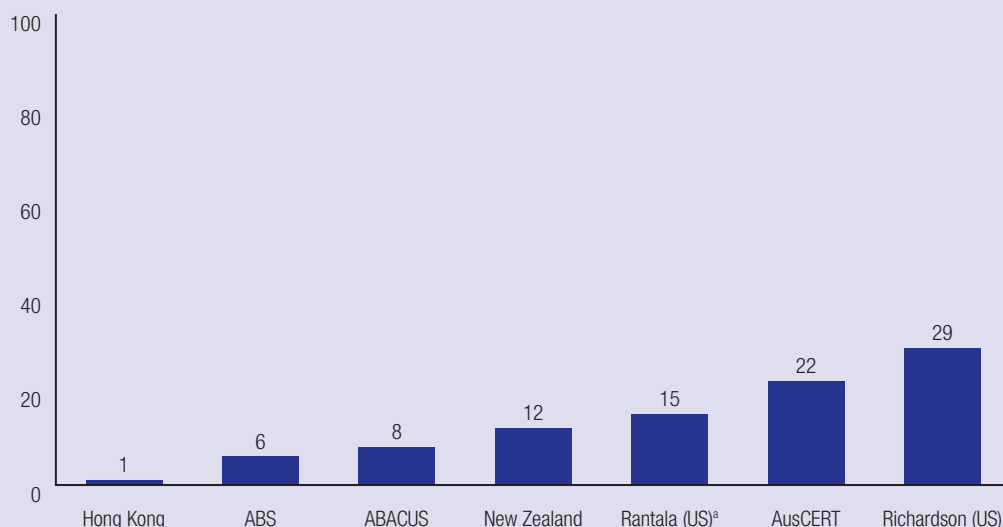
Large businesses are more likely than small or medium businesses to have dedicated information technology security specialists or teams within their organisation. As such, large organisations may be privy to more knowledge or greater awareness of external reporting options than small or medium businesses.

Interestingly, although the ABACUS data indicate that of businesses with information technology, large businesses (88%) are more likely than medium (80%) or small (59%) businesses to have an insurance plan that covers one or more computer security incidents,

the data also show that of these businesses, large businesses (63%) are less likely than medium (74%) or small (86%) businesses to have an insurance requirement that they report computer security incidents to the police. As such, insurance requirements can be excluded as an explanation for large businesses' higher incidence of reporting computer security incidents to third parties. Levels of reporting for insurance reasons should not be considered a reflection of businesses' perceived seriousness of the offence, or perception of victimisation, but associated with an administrative requirement.

The ABACUS data indicate that in relation to businesses that have experienced one or more computer security incidents, large businesses are more likely than medium businesses and medium businesses more likely than small businesses to report computer security incidents to police, non-police enforcement or regulatory agencies and external computer security incident response teams. Small victimised businesses (78%) were more likely than medium (74%) and large (72%) victimised businesses to deal with their most significant computer security incident internally,

Figure 30 Victimised businesses that reported computer security incidents to law enforcement, comparison with other surveys (percent)



a: Law enforcement was broadly defined in this survey and included CERT CC (a computer emergency response team).

Note: ABACUS n=766. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience any computer security incidents and 46 missing answers (40 from small, 6 from medium, 1 from large businesses). Hong Kong n=unknown. ABS n=unknown. New Zealand n=25. Rantala n=unknown. AusCERT n=165. Richardson n=274.

Source: AIC, ABACUS 2008 [computer file, weighted data]

without involving external third parties. These findings again suggest a relationship between business size and reporting behaviours following a computer security incident, with smaller businesses generally more likely to deal with computer security incidents internally, and larger businesses more likely to involve external agencies. This relationship does not appear to exist, however, in relation to reporting incidents to lawyers or electronic payment providers.

The above findings support some of the existing data on reporting behaviours following computer security incidents against businesses. In Australia, the ABS (2007: 13) *Business Use of Information Technology* survey found that 76 percent of victimised businesses dealt with computer security incidents inside the business and six percent reported the incident to a law enforcement agency. One percent of respondents reported the incident to a lawyer, six percent took an 'other' action and 16 percent took no action.

AusCERT's most recent survey found that 69 percent of victimised businesses did not report computer security incidents outside of

their business, seven percent reported to the Australian High Tech Crime Centre, 22 percent reported to police or other Australian law enforcement authority, 15 percent to a computer security incident response team such as AusCERT and 10 percent to a lawyer. The higher proportion of respondents to the AusCERT survey that reported incidents to a computer security incident response team might perhaps be explained by AusCERT's sample being partly drawn from the TISN, members of which may be more familiar with the work of AusCERT than the broader business community.

Results from some international surveys also reflect those of the ABACUS research. New Zealand's computer security survey (Quinn 2006), for example, found that 52 percent of victimised businesses did not report computer security incidents to external agencies. Twelve percent reported incidents to the police and four percent to a lawyer. A survey of Hong Kong businesses by Broadhurst et al. (2006) similarly found a high proportion of businesses not reporting computer security incidents to any external agency (84%). Six percent of Hong Kong

respondents reported incidents to an Internet Service Provider (ISP), five percent to 'someone else', four percent to a systems administrator and one percent each to a law enforcement agency and a website administrator. Rantala (2008: 1) found that 80 percent of victimised businesses dealt with computer security incidents within their organisation, 15 percent reported to an external organisation and 15 percent to law enforcement authorities. Interestingly, Rantala (2008: 2) found that 'cyber thefts' were far more likely to be reported to the police than other types of computer security incident. This may be the case because such thefts more closely reflect traditional larceny offences and are more likely to be viewed by victims as 'real' crimes. Cyber thefts may also result in more tangible outcomes than other computer security incidents. This may also make them more likely to be reported to law enforcement authorities.

As shown in Figure 31, Richardson's (2007) survey of businesses in the United States produced results that vary considerably from those outlined above. Richardson (2007: 22) found that respondents were almost as likely to report a computer security incident to law enforcement (29%) as not report the incident to any external agency (30%). These findings differ considerably from both the ABACUS survey results and those of the other international studies outlined above. Respondents to Richardson's (2007) survey were more likely to have reported computer security incidents to law enforcement authorities and less likely to have dealt with incidents without involving external agencies. This may be due to a number of reasons.

Richardson's (2007) study sampled businesses associated with the Computer Security Institute, rather than the general business population. It is possible, therefore, that respondents had a greater security consciousness than the general population of businesses. As a result, these respondents may possess a greater awareness of computer security incident legislation and reporting options.

Cultural differences may also partially explain this difference in findings between the United States, the Antipodes and Hong Kong. It is thought, for example, that the United States has a particularly litigious culture compared with most other nations. This may encourage higher levels of reporting of computer security incidents.

Importantly, the New Zealand, Hong Kong and US surveys asked respondents broader questions around 'actions taken' following computer security incidents than the ABACUS survey, which focused more narrowly on reporting behaviours following computer security incidents. Actions other than reporting to external agencies dominated responses in those surveys where other actions were included as potential responses. In New Zealand, the most common response to a question about 'actions taken' following computer security incidents was 'patched security holes'. Eighty-eight percent of respondents selected this response (Quinn 2006: 11). Respondents to Richardson's (2007: 22) US survey selected 'attempted to identify perpetrator' (61%), 'did your best to patch security holes' (54%), 'installed security patches' (48%) and 'installed additional security software' (36%) among other responses to a question about 'action taken' following computer security incidents.

Although respondents to the ABACUS survey were not given any of these options, respondents could select the 'other' option and identify an alternative response to the survey's question about reporting behaviour. Eleven percent of respondents selected 'other' in response to the ABACUS survey's question about reporting behaviours following a business's most significant computer security incident. Of this 11 percent, 38 percent reported the computer security incident to an information technology company, consultant or department, 25 percent reported the incident to a vendor, 15 percent reported to a bank or insurance company, six percent upgraded their computer security measures and three percent took no action. It is important to be aware when interpreting these results that these percentages represent very small numbers of businesses.

As outlined above, in surveys where some of these options were listed, they were selected by large proportions of respondents. In contrast, in the survey by Broadhurst et al. of Hong Kong businesses, only small percentages of respondents reported incidents to ISPs, website administrators and systems administrators (see above). It is therefore impossible to suggest what proportion of respondents may have selected options such as these had they been listed on the ABACUS survey. It is nonetheless important to note this difference among surveys.

There are a number of factors that may contribute towards low levels of reporting to external third parties. Computer-facilitated crimes can lack the personal affront that accompanies other crimes. Offenders are usually faceless and victims often believe that they have not been personally selected or attacked. In the ABACUS survey, 44 percent of small businesses, 38 percent of medium businesses and 32 percent of large businesses that had experienced computer security incidents identified not having been explicitly targeted as a reason their business's most significant computer security incident was not reported to a third party. This suggests that victims of computer security incidents may feel that they have not 'really' been victimised. In Rantala's (2008: 7) report on computer security incidents against businesses in the United States, 22 percent of businesses 'did not think to report' such incidents. Twenty-one percent of victimised businesses in the ABACUS survey similarly did not think to report the incident. This again suggests that those affected by computer security incidents may not feel personally targeted or victimised.

Victims of particular types of computer security incidents, such as phishing scams, are often labelled 'gullible', 'greedy' or even 'stupid' (e.g. see Stolz 2008). This may also impact on levels of reporting of computer security incidents. Fear of being considered greedy or gullible may prevent victims of computer security incidents perceiving themselves as real victims, and as such, reduce the number of victims who report incidents, seek assistance and/or proceed with prosecutions.

The uncertainty surrounding who is responsible for preventing and/or responding to computer security incidents is another factor that may influence businesses' decisions to report security incidents. According to CyberSource (2008: 19), consumers polled on who should accept responsibility for online fraud list retailers, ISPs and credit card companies before the police. In contrast, retailers themselves believe that the police are not doing enough (CyberSource 2008: 19). Australian music industry representatives have recently called for greater responsibility from ISPs to help stem illegal music downloading (Shedden 2008). This type of strategy not only makes it unclear who is responsible for responding to computer security incidents, but potentially reinforces the notion that these sorts

of actions aren't really crimes, since they are not dealt with by law enforcement authorities. This could potentially lead to a vicious cycle of under-reporting, whereby victims of computer security incidents do not report offences as they are not seen as crimes, and law enforcement agencies do not respond effectively to these incidents because victims under-report them, or report them to non-law enforcement agencies.

Finally, it is important to consider the significant financial, temporal and other costs that reporting computer security incidents may incur. Issues relating to financial costs, the time taken to report incidents and emotional and personal costs are commonly listed by victims of terrestrial crimes as reasons why they choose not to report offences to the police. These factors may also impact on businesses' decisions about reporting computer security incidents.

Satisfaction with reporting of computer security incidents

The ABACUS survey asked respondents to rate their satisfaction with the outcome of their reporting decisions following their businesses' most significant incident. Sixty-seven percent of respondents that dealt with their most significant computer security incident internally reported being either 'satisfied' or 'very satisfied' with the outcome. Slightly lower proportions of businesses that reported their most significant computer security incident to an electronic payment provider (60%), a computer emergency response team (55%) or a non-police/regulatory agency (52%) reported being 'satisfied' or 'very satisfied' with the outcome. Forty-three percent of those reporting to police were 'satisfied' or 'very satisfied' and 33 percent were 'neither satisfied nor dissatisfied'. Only 18 percent of those reporting to a lawyer were 'satisfied' or 'very satisfied' and 23 percent were 'neither satisfied nor dissatisfied'. These findings must be interpreted cautiously, however, due to the small numbers of respondents that reported their most significant computer security incident externally.

Businesses' reasons for not reporting computer security incidents

A variety of reasons are put forward in the literature on computer security incidents against businesses as to why businesses commonly deal with incidents internally and do not report them to external parties. Reasons commonly given for not reporting incidents include:

- considering the offence too trivial or not worth reporting
- not having enough time to make a complaint
- believing that there is little chance of a successful prosecution
- a lack of evidence
- believing that police wouldn't be interested
- fear of negative publicity
- wanting to deal with the matter internally
- fearing that reporting would result in competitor advantage
- preferring to pursue a civil remedy.

Respondents that reported that their business's most significant computer security incident had not been referred to an external third party, but had been dealt with internally, were asked to list the reasons their business chose not to report the incident. The most common reasons given by respondents to the ABACUS survey were the incident not being serious enough to report (48%), preferring to deal with the incident internally (46%), the business not being explicitly targeted (43%) and a perception that there was nothing to gain from reporting the incident to an external third party (38%). Twenty-one percent of respondents did not think to report their business's most significant computer security incident, 17 percent did not know who to contact, nine percent felt the incident was outside the jurisdiction of law enforcement and six percent did not know the reason their business's most significant incident had not been reported to an external agency. Small proportions did not want data or hardware seized as evidence (2%), feared reprisals (1%) or repeat victimisation (1%), or felt that competitors would use the incident to their advantage (<1%).

As indicated in Table 43, considerable proportions of small (44%), medium (57%) and large (56%)

victimised businesses reported that dealing with the incident internally was, in and of itself, a reason for not reporting incidents to an external party.

Negative publicity is frequently listed as an important reason that informs businesses' decisions not to report computer security incidents (see Hughes & DeLone 2007; Webroot Software 2008b). As indicated in Figure 31, considerably higher proportions of respondents to previous surveys on computer security incidents against businesses listed negative publicity as a factor in their decisions not to report computer security incidents than did respondents to the ABACUS survey.

Table 43 Victimised businesses' reasons for not reporting most significant computer security incident to an external party, by business size (percent)

	Small	Medium	Large	Weighted n
Negative publicity	1	0	7	1
Business was not explicitly targeted e.g. worm	44	38	32	251
Nothing to gain	39	32	50	222
Did not think to report	22	14	12	122
Incident outside jurisdiction of law enforcement	9	9	2	50
Did not want data or hardware seized as evidence	2	0	3	10
Did not know who to contact	19	9	4	101
Incident not serious enough to report	49	43	27	283
Competitors would use to their advantage	<1	0	0	1
Dealt with internally	44	57	56	267
Fear of reprisals	1	0	3	7
Fear of repeat victimisation	1	0	0	6
Other	1	0	3	3
Don't know	6	6	8	37

Note: n=587. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience a computer security incident, 176 businesses that reported computer security incidents externally and 49 missing answers (46 from the previous question on reporting behaviours following the most significant computer security incident)

Source: AIC, ABACUS 2008 [computer file, weighted data]

The ABACUS data suggest that for Australian businesses, negative publicity was not an important factor in decisions about whether to report computer security incidents to third parties. Just one percent of victimised businesses identified negative publicity as one of the reasons they did not report their most significant computer security incident. Reasons listed more commonly by victimised businesses were the incident not being serious enough to report (48%), preferring to deal with the incident internally (46%), the business not being explicitly targeted (43%) and a perception that there was nothing to gain from reporting the incident to an external third party (38%).

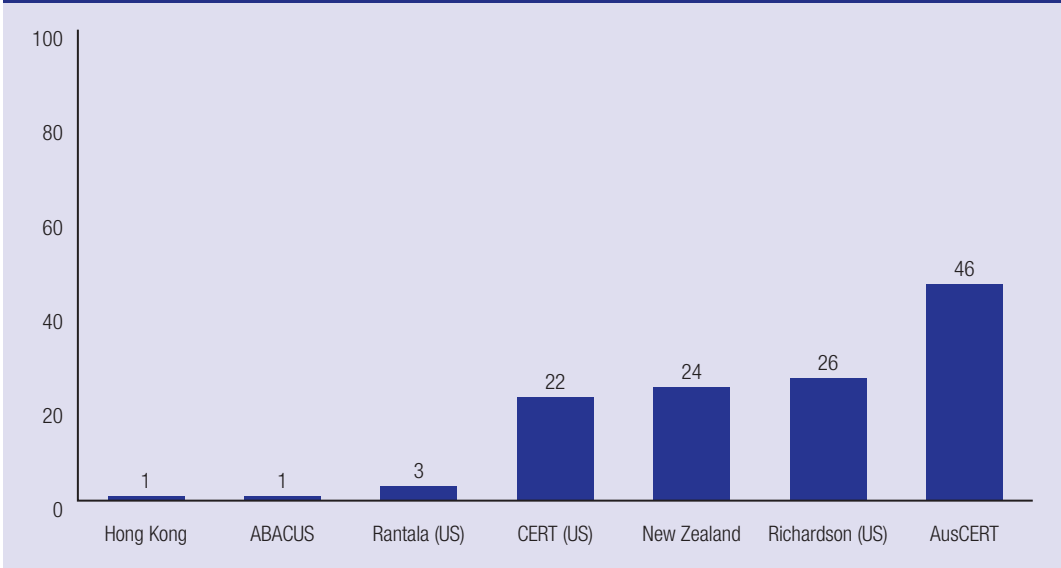
Interestingly, respondents to Hong Kong's survey were also asked to indicate the reason their business *did* choose to report computer security incidents to third parties. Responses included: crimes should be reported/serious event (38%), other reason (35%), to stop it happening again (16%), to recover property (8%), wanting the offender to be caught/punished (5%) and insurance reasons (3%; Broadhurst et al. 2006).

The difference among surveys in this regard is striking. It may be the result of a number of factors.

- As already discussed, the ABACUS survey's representative sample and use of weighted data reflect the entire population of businesses in Australia. It is somewhat unsurprising that surveys that sampled only large businesses, businesses with higher annual turnovers or businesses from the computer security industry found higher proportions listing negative publicity as a factor in their decisions not to report computer security incidents.
- The ABACUS survey also excluded government organisations from its sample, whereas these were included in some previous surveys. It is reasonable to assume that negative publicity may be an important factor for government organisations. This may also have affected the ABACUS study's finding of a smaller proportion of businesses concerned about negative publicity.

It is important to note, additionally, that Rantala's (2008: 7) survey found a similar proportion of businesses citing negative publicity as a reason

Figure 31 Victimised businesses that listed negative publicity as a reason for not reporting computer security incidents to external agencies, comparison with other surveys (percent)



Note: n=587. Excludes 307 businesses with no information technology, 2,881 businesses that did not experience a computer security incident, 176 businesses that reported computer security incidents externally and 49 missing answers. Hong Kong n=unknown. Rantala n=unknown. CERT n=unknown. New Zealand n=25. Richardson n=196. AusCERT n=130

Source: AIC, ABACUS 2008 [computer file, weighted data]

Businesses
do not
perceive
the police
as the most
appropriate
agency to
report to

for not reporting computer security incidents to the police. Like the ABACUS survey, Rantala's (2008) survey used a random, stratified sample of businesses and a large sample size. It is therefore possible that other surveys have overstated the importance of negative publicity in informing businesses' decisions about reporting computer security incidents.

Finally, it is important to consider to what extent reporting to law enforcement authorities represents the most appropriate response by businesses that have experienced a computer security incident. While the ABACUS data clearly indicate that businesses do not perceive the police as the most appropriate agency to report to, it may also be the case that law enforcement agencies do not have the capacity to deal with every computer security incident affecting businesses across Australia. As the ABACUS data clearly indicate, businesses that deal with computer security incidents without reporting them to an external agency are overwhelmingly satisfied with their reporting decisions.



Conclusion

Summary of key findings

The ABACUS study was the first nationwide survey of its kind in Australia. It randomly sampled small, medium and large businesses across all industry sectors and weighted data to more accurately reflect the business community. The study has presented an empirical investigation of the prevalence and nature of computer security incidents against businesses in Australia. The study's findings should be considered as a contribution to the evidence on computer security incidents against businesses and may be used to inform further research in this area. After briefly summarising the study's key findings, this section will outline some implications of the ABACUS project's findings.

Preventing computer security incidents against businesses

A majority of businesses used at least one computer security tool to prevent computer security incidents, with anti-virus software being the most commonly used. Fewer than half of businesses used computer security policies.

A clear relationship was found between the use of computer security tools and policies and business size, with larger businesses using more security tools and policies than smaller businesses. Similar

proportions of businesses used computer security tools across all industry sectors. The lowest proportion was in the construction sector, with 79 percent of businesses using computer security tools, and the highest proportion was in both financial and insurance services and education and training (both 92%). In general, higher proportions of businesses with higher annual turnovers used computer security tools.

Reasonably similar proportions of businesses used computer security policies across all business sectors. Use of computer security policies ranged from 26 percent in agriculture, forestry and fishing to 57 percent in education and training businesses. A clear relationship was found between the annual turnover of a business and the use of computer security policies, with lower proportions of businesses with lower annual turnovers using computer security policies.

Smaller proportions of businesses reported using almost all computer security tools and policies than respondents to previous surveys have done.

Prevalence of computer security incidents against businesses

Fourteen percent of businesses experienced one or more computer security incidents. A relationship was

found between business size and the number of incidents experienced, with larger businesses experiencing more incidents than smaller businesses. A relationship was also apparent between businesses' annual turnover and the number of incidents experienced, with greater proportions of businesses with a higher annual turnover experiencing computer security incidents than those with a lower annual turnover.

Previous surveys in Australia and New Zealand have found similar levels of computer security incidents against businesses. The ABACUS study found lower levels of computer security incidents against businesses than previous studies in the United States have found.

Nature of computer security incidents against businesses

Viruses and other malicious code were the computer security incident experienced by the highest proportion of businesses and ranked by the highest proportion of respondents as the most significant computer security incidents affecting their business. Higher proportions of smaller businesses reported experiencing viruses and other malicious code than larger businesses, although a clear relationship between business size and types of computer security incidents experienced was not found in the ABACUS study. Reasonably even proportions of businesses from each industry sector experienced each type of computer security incident.

Impacts of computer security incidents against businesses

The majority of businesses experienced some type of negative impact following their most significant computer security incident, with corruption of hardware or software being the most common outcome. Businesses size was found to be related to whether businesses experienced any effects following their most significant computer security incident, with higher proportions of large businesses reporting negative impacts.

Responding to computer security incidents against businesses

A majority of businesses from all sectors dealt with their most significant computer security incident internally and did not report the incident to any third party. Reporting behaviours did not vary greatly across industry sectors or by businesses' annual turnover. Eight percent of businesses reported their most significant computer security incident to the police. The most common reason given for not reporting their most significant incident was that the incident was not serious enough to report.

Some implications of key ABACUS findings

A number of implications stem from the key findings of the ABACUS survey. Although it would be impossible to cover all of these in detail, some of the major implications are outlined below.

Under-reporting of computer security incidents against businesses

It is widely accepted in the literature that businesses are unlikely to report incidents to law enforcement authorities (Hughes & DeLone 2007: 82; Wall 2007: 194). This is usually viewed as the result of businesses' fear of negative publicity: 'in the commercial sector, fear of the negative impact of adverse publicity greatly reduces their willingness to report their victimisation to the police' (Wall 2007: 194).

The ABACUS data indicate that overall, few businesses report computer security incidents to law enforcement authorities. Only eight percent of businesses surveyed reported their most significant incident to the police. The ABACUS data therefore support the perception that businesses report only a small percentage of computer security incidents. This proportion varied considerably by business size, however, with seven percent of small, 14 percent of medium and 21 percent of large businesses reporting their most significant computer security incident to the police.

That large businesses are most likely to report computer security incidents to the police is, on one level, somewhat unsurprising. Large businesses suffer greater financial losses and are likely to have more specialised information technology staff with better information technology knowledge. It is likely, therefore, that large businesses are more aware of reporting options and have greater reasons to report computer security incidents to law enforcement authorities.

In contrast with findings from previous studies of computer security incidents against businesses, the ABACUS project found that only one percent of businesses listed 'fear of negative publicity' as a reason for not reporting computer security incidents to external agencies such as the police or a lawyer. This also varied by business size, with large businesses more likely than medium or small businesses to list fear of negative publicity as a factor in their decision-making regarding reporting computer security incidents.

Importantly, however, businesses that may have more to lose via negative publicity (i.e. large businesses) were also more likely to report computer security incidents to law enforcement authorities. These findings challenge the perception that negative publicity is a primary concern of businesses victimised by computer security incidents.

The ABACUS data support what Wall (2007: 191) calls the 'de minimis trap'—that is, the perception that the law 'does not deal with trifles'. Businesses in the ABACUS survey listed the incident not being serious enough to report as the major reason they did not report computer security incidents to external agencies. These data therefore strongly suggest that the 'de minimis trap' plays a role in businesses' decisions about whether to report computer security incidents. The ABACUS data also strongly support Wall's (2007: 195) claim that computer security incidents are rarely reported to police simply because they are effectively dealt with by victims themselves. The ABACUS data clearly show that a majority of businesses deal with computer security incidents internally, without reporting these to external agencies. Additionally, a substantial proportion of businesses (46%) reported that dealing with computer security

incidents internally was, in and of itself, a reason for not reporting these incidents externally. Moreover, the highest proportion of businesses that reported being 'satisfied' or 'very satisfied' with the outcome of the action they took following their most significant computer security incident (67%) were those that dealt with the incident internally. The ABACUS data therefore strongly suggest that in the main, businesses do not view computer security incidents as serious enough to report to police and are satisfied with the outcomes of dealing with computer security incidents internally. These findings highlight the marginal role played by law enforcement authorities in responding to computer security incidents against businesses.

It is widely accepted that those who perpetrate computer security incidents are unlikely to be detected and/or punished for their crimes. Criminologists have long argued that the *certainty* of punishment, rather than the *severity* of punishment, prevents would-be criminals more effectively. In the case of computer crimes, which are very difficult to police (Walker et al. 2006; Wall 2007) and prosecute (Brenner 2006; Grabosky 2007; Urbas & Choo 2008; White & Fisher 2008), there is often neither the threat of punishment nor any likelihood of detection to facilitate prevention. Low levels of reporting may contribute to this problem and help perpetuate a cycle of under-reporting and under-policing.

Low reporting levels for computer security incidents may help advance the perception that law enforcement responses are ineffective in dealing with these sorts of crimes. This may, in turn, result in business users of information technology being made responsible for preventing and/or responding to computer security incidents independently of law enforcement and other external agencies. The ABACUS data suggest that to a large extent this is currently the case, with small, medium and large businesses dealing with a high proportion of computer security incidents internally. This means that not only do businesses have to deal with the consequences of computer security incidents themselves, but that the extent of these incidents will continue to remain hidden.

It may also be important to consider the substantial costs associated with reporting computer security incidents. Surveys and other literature on computer

security incidents against businesses usually fail to consider the financial, temporal and even emotional costs that may be involved in reporting computer security incidents to police. Victims of 'terrestrial' crimes often list these as important factors that inform their decision not to report offences to the police. It is therefore reasonable to assume that the various costs involved in reporting computer security incidents may influence businesses' decisions not to report these incidents to external agencies.

Theft of personal details

The literature on computer security incidents against businesses has, in recent years, highlighted the increased attractiveness of personal data as a target for cyber criminals (Choo 2008; Choo, Smith & McCusker 2007a; Georgia Tech Information Security Center 2008; Wall 2007). Personal data may be targeted as they can be used to facilitate identity theft (Choo, Smith & McCusker 2007a: 52) and other online frauds (Choo 2008). Businesses may therefore be lucrative targets as their information technology systems often hold large volumes of customer or client details. Businesses in the retail, healthcare and/or education sectors, for example, are likely to store large quantities of personal details in information technology systems.

It is therefore important to consider the types of computer security incidents against businesses that may facilitate identity theft. The ABACUS study found high proportions of businesses experiencing computer security incidents such as viruses and other malicious code, theft or loss of hardware, unauthorised network access and phishing. These computer security incidents could facilitate the theft of personal data and therefore 'be the precursor to more serious crimes' (Wall 2007: 186). One recent report (cited in Choo 2008: 274) noted, for example, that 'most new malware is designed to steal financial data (e.g. credit card details, bank account details, passwords, PIN numbers) as a precursor to various frauds and other deceptions' (see also Georgia Tech Information Security Center 2008).

Although these types of computer security incidents were experienced by large proportions of ABACUS respondents, there is no way of knowing whether personal data were stolen and used to facilitate

further offences. Symantec (2007: 12) argue, for example, that often:

Theft or loss of a computer or computer media is driven not by a desire to steal data, but to steal the hardware itself. A person who steals a laptop is likely driven by the desire to simply sell the laptop for financial gain, and not to harvest the data it may store.

Nonetheless, it is important to be aware of the possibility that personal data may be the intended target of a range of computer security incidents against businesses. Of particular concern is the finding in the ABACUS study that only 11 percent of businesses reported using policies aimed at protecting electronic information such as customer account details.

Although it is impossible to ascertain the extent of the problem of personal data being targeted by cyber criminals, this is important to be aware of when interpreting ABACUS and other data on computer security incidents that may feed into identity theft and related offences.

Cybercrimes and cyber criminals

The ABACUS research study generated rich data that can be used to assess the image of cybercrimes and cyber criminals portrayed in the literature on computer security incidents against businesses.

It is widely accepted in the literature that cyber criminals are increasingly organised (Cooper 2006: 6; Sophos 2008: 1; Websense 2006: 1) and sophisticated (Kerr 2007: 21; Wilkins 2006: 16). Computer security incidents are portrayed as being increasingly targeted at particular organisations (Kerr 2007: 21; Symantec 2006: 4; Wilkins 2006) and financially motivated (Choo 2008; Phair 2007: 6; Sophos 2008: 1; Symantec 2006: 4; Websense 2006: 1; Wilkins 2006: 16). Additionally, cyber criminals are portrayed in the literature as able to be increasingly anonymous (Kerr 2007: 1; Phair 2007: 6).

It appears that businesses share this perception about the changing face of cybercrime and cyber criminals and the threat they represent. Eighty percent of Australian organisations surveyed

by Ho (2006: 11) agreed with the statement that 'lone hackers are increasingly being replaced by organized criminal groups that are adopting technical sophistication'. Research by CyberSource (2006: 9) found that 39 percent of business respondents felt threatened by a perceived increase in the sophistication of fraudsters. Deloitte Touche Tohmatsu (2006: 13) capture the perceived shift in the nature of perpetrators of computer security incidents as follows:

Financially motivated, targeted attacks are increasing and the criminal profile is shifting—from script kiddies and disorganized hackers to well funded organized crime rings, whose around-the-clock, across-the-globe attacks are yielding big financial payback....The attackers are transitioning from mass virus and worm attacks to attract attention and publicity to stealthier methods to avoid detection.

Comments of this nature, which stress the changing nature and increasing threat of computer security incidents and those who perpetrate them, are typical in the literature on this topic, particularly in reports from vendors and in the literature targeted towards industry professionals (Intersec 2006; Kerr 2007; Pang 2006; Wilkins 2006).

At the same time, however, the literature portrays cyber criminals as requiring fewer technological skills than ever before (Phair 2007: 6; Websense 2006: 1). McAfee (2007: 25), for example, states that 'computer skills are no longer necessary to execute cybercrime'. Two conflicting depictions of perpetrators of computer security incidents therefore co-exist in the literature on this topic.

Perpetrators of computer security incidents are also contradictorily portrayed as both opportunistic and predatory. The industry-specific literature highlights the increasingly predatory nature of emerging computer security threats such as 'spear phishing' or 'whaling' (Choo 2008: 274), in which 'criminals bombard businesses with highly-targeted spam that appears to have originated from within the organisation' (Wilkins 2006: 16). Simultaneously, however, perpetrators are portrayed as operating in an ad hoc, opportunistic manner.

Where once a cyber criminal had to have superior computing knowledge, there are now so many vulnerabilities to be exploited, freely available from

search engines, that the motivations of these types of criminals may be significantly different, depending upon their skill levels (Phair 2007: 6).

Two 'classes' of cyber criminals are depicted in the literature, whereby 'minimal skill is needed for opportunistic attacks [yet] targeted attacks require more sophisticated skills' (Kshetri cited in Choo 2008: 276).

In general, the ABACUS data appear to support the image of cyber criminals as opportunistic actors perpetrating random attacks, rather than predatory actors carrying out targeted attacks. As described earlier in this report, relatively even proportions of businesses from each industry sector reported experiencing computer security incidents. Although more large businesses than medium or small businesses reported experiencing computer security incidents, this may reflect the more widespread use of information technology among larger businesses, or a greater awareness of computer security incidents, as discussed earlier. These findings may challenge the commonly-held view that financial organisations and large businesses are 'better' or more likely targets for cyber criminals.

Viruses and other malicious code were the most commonly experienced computer security incidents by businesses in the ABACUS study. Computer security incidents that are likely to be targeted, such as denial of service, sabotage of network or data and incidents involving businesses' web applications, were experienced by only very small proportions of ABACUS respondents. The computer security incidents that have the most impact (financial and otherwise) on businesses in the ABACUS research therefore do not appear to have been targeted.

Opportunity might therefore be considered a primary motivating factor behind criminals' decisions to perpetrate computer security incidents against businesses. As stated above, criminologists have long argued that it is the certainty of detection, rather than the severity of punishment, that deters would-be criminals. In the case of computer security incidents against businesses, where the chances of detection are very low, perpetrators certainly appear to be acting on opportunities to commit offences. This has important implications for future policy in this area.

The ABACUS study was the first of its kind in Australia

Future research directions

The ABACUS study was the first of its kind in Australia. It presented a nationwide empirical study of the prevalence, nature and effects of computer security incidents against businesses. The key findings of the research, summarised above, should be considered a contribution to the evidence base on computer security incidents against businesses in Australia and internationally. These findings should form part of the platform from which future research in this area might be developed. Future research may, for example, consider:

- How businesses identify computer security incidents, and specifically, how they distinguish technical failures from criminal acts
- What informs businesses' approaches to computer security
- Whether and how computer security incidents involving personal data are used in the commission of future crimes such as identity fraud
- The reasons businesses choose to report computer security incidents
- Whether and how legislation in various jurisdictions has impacted on the prevalence, nature and effects of computer security incidents against businesses
- Whether and how businesses' approaches to computer security affect consumer behaviour.



References

All URLs were correct on 16 October 2008

Allan G 2005. Responding to cybercrime: a delicate blend of the orthodox and the alternative. *New Zealand law review* 2: 149–178

Anti-Phishing Working Group 2008. *Phishing activity trends: report for the month of January, 2008*. http://www.antiphishing.org/reports/apwg_report_jan_2008.pdf

Australian Bureau of Statistics (ABS) 2007. *Business use of information technology 2005–06*. ABS cat. no. 8129.0. Canberra: ABS

Australian Bureau of Statistics & Statistics New Zealand 2006. *Australian and New Zealand standard industrial classification 2006*. cat. no. 1292.0. Canberra: ABS

Australian Communications and Media Authority (ACMA) 2008. *Developments in internet filtering technologies and other measures for promoting online safety*. Canberra: ACMA

Australian Communications and Media Authority (ACMA) 2007. *Telecommunications today: consumer attitudes to take-up and use*. Canberra: ACMA

Australian Computer Emergency Response Team (AusCERT) 2008. *Home users computer security survey 2008*. Brisbane: AusCERT

Australian Computer Emergency Response Team (AusCERT) 2006. *2006 Australian computer crime and security survey*. Brisbane: AusCERT

Australian Institute of Criminology (AIC) 2006a. Malware—viruses, worms, Trojan horses. *High tech crime brief* no. 10. Canberra: AIC. <http://www.aic.gov.au/publications/htcb/htcb010.html>

Australian Institute of Criminology (AIC) 2006b. More malware—adware, spyware, spam and spim. *High tech crime brief* no. 11. Canberra: AIC. <http://www.aic.gov.au/publications/htcb/htcb011.html>

Australian Institute of Criminology (AIC) 2005. Concepts and terms. *High tech crime brief* no. 1. Canberra: AIC. <http://www.aic.gov.au/publications/htcb/htcb001.html>

Brenner S 2007. 'At light speed' attribution and response to cybercrime/terrorism/warfare. *Journal of criminal law and criminology* 97(2): 379–475

Brenner S 2006. Cybercrime jurisdiction. *Crime, law and social change* 46: 189–206

Broadhurst R et al. 2006. *Preliminary report of the international crime victimisation survey, 2005*. Hong Kong: Social Science Research Centre, Hong Kong University

Challice G 2008. *The Australian business assessment of computer user security (ABACUS) survey: methodology report*. Canberra: AIC

Choo R 2008. Organised crime groups in cyberspace: a typology. *Trends in organized crime* 11(3): 270–295


Choo R, Smith R & McCusker R 2007a. *Future directions in technology-enabled crime: 2007–09*. Research and public policy series no. 78. Canberra: AIC. <http://www.aic.gov.au/publications/rpp/78/index.html>

Choo R, Smith R & McCusker R 2007b. The future of technology-enabled crime in Australia. *Trends & issues in crime and criminal justice* no. 341. Canberra: AIC. <http://www.aic.gov.au/publications/tandi2/tandi341.html>

- Computer Emergency Response Team, US Secret Service, CSO Magazine and Microsoft 2007. *2007 e-crime watch survey*. http://www.cert.org/search_pubs/search.php
- Cooper C 2006. Combating the cyber-crooks. *Australian law management journal*. Winter: 6–8
- CyberSource 2008. *Fourth annual UK online fraud report: online payment fraud trends, merchant and consumer response*. Reading: CyberSource
- CyberSource 2006. *Second annual UK online fraud report: online payment fraud trends and merchants' response*. Reading: CyberSource
- Darrow B 2008. Is your CEO a cybercrime target? *Computerworld* January: 30: 32–33
- Deloitte Touche Tohmatsu 2007. *2007 global security survey*. London: Deloitte Touche Tohmatsu
- Deloitte Touche Tohmatsu 2006. *2006 global security survey*. London: Deloitte Touche Tohmatsu
- Department of Trade and Industry 2006. *Information security breaches survey 2006: technical report*. London: Department of Trade and Industry
- Georgia Tech Information Technology Center 2008. *Emerging cyber threats report for 2009: data, mobility and questions of responsibility will drive cyber threats in 2009 and beyond*. Atlanta, GA: Georgia Tech Information Technology Center
- Grabosky P 2007. Requirements of prosecution services to deal with cyber crime. *Crime, law and social change* 47(4/5): 201–223
- Ho A 2006. *Global business security survey: key highlights*. http://business.singtel.com/upload_hub/singtel_hk/EB-IBM.pdf
- Hughes L & DeLone G 2007. Viruses, worms, and trojan horses: serious crimes, nuisance, or both? *Social science computer review* 25(1): 78–98
- IBM Global Technology Services 2008. *IBM internet security systems x-force 2007 trend statistics*. Somers, NY: IBM Corporation
- Intersec 2006. Behind the keys. *Intersec* November/December: 31–33
- Jones B 2007. Comment: virtual neighborhood watch: open source software and community policing against cybercrime. *Journal of criminal law & criminology* 97(2): 601–629
- Kerr J 2007. Cyber crime battle. *Australian national security magazine* February: 21–23
- Marron D 2008. 'Alter reality': governing the risk of identity theft. *British journal of criminology* 48(1): 20–38
- McAfee 2007. *Cybercrime: the next wave*. Santa Clara, CA: McAfee
- McCusker R 2006. Transnational organised cyber crime: distinguishing threat from reality. *Crime, law and social change* 46: 257–273
- Nykodym N, Taylor R & Vilela J 2005. Criminal profiling and insider cyber crime. *Computer law & security report* 21: 408–414
- Pang B 2006. Fighting cyber-crime through global partnerships. *Royal Canadian mounted police gazette* 68(3): 34–35
- Parliamentary Joint Committee on the Australian Crime Commission 2004. *Cybercrime*. Canberra: Parliament of the Commonwealth of Australia
- Phair N 2007. *Cybercrime: the reality of the threat*. ACT: Nigel Phair
- Quinn KJ 2006. *Second annual New Zealand computer crime and security survey*. Dunedin: Alpha-Omega Group
- Rantala R 2008. *Bureau of justice statistics special report: cybercrime against businesses, 2005*. Washington DC, USA: Bureau of Justice Statistics
- Richardson R 2007. *2007 CSI computer crime and security survey*. San Francisco, CA: Computer Security Institute
- Rollings K 2008. *Counting the costs of crime in Australia: a 2005 update*. Research and public policy series no. 91. Canberra: AIC. <http://www.aic.gov.au/publications/rpp/91/index.html>
- Smith R 2007. Crime control in the digital age: an exploration of human rights implications. *International journal of cyber criminology* 1(2): 167–179
- Smith R, Grabosky P & Urbas G 2004. *Cyber criminals on trial*. Cambridge: Cambridge University Press
- Sophos 2008. *Security threat report 2008*. Boston, MA: Sophos
- Stolz G 2008. *Expert to tackle cybercrime out of Africa*. <http://www.news.com.au/couriermail/story/0,23739,23735684-3102,00.html>
- Symantec 2008. *Symantec internet security threat report: trends for July – December 07*. Cupertino, CA: Symantec
- Symantec 2007. *Symantec internet security threat report: trends for January – June 07*. Cupertino, CA: Symantec
- Symantec 2006. *Symantec internet security threat report: trends for January 06 – June 06*. Cupertino, CA: Symantec
- Urbas G & Choo R 2008. *Resource materials on technology-enabled crime*. Technical and background paper series no. 28. Canberra: AIC <http://www.aic.gov.au/publications/tbp/tbp028/tbp028.pdf>
- Walker D, Brock D & Stuart T 2006. Faceless-oriented policing: traditional policing theories are not adequate in a cyber world. *The police journal* 79(2): 169–176

- Wall D 2007. Policing cybercrimes: situating the public police in networks of security within cyberspace. *Police practice and research: an international journal* 8(2): 183–205
- Webroot Software 2008a. *State of internet security: protecting consumers online*. Boulder, CO: Webroot Software
- Webroot Software 2008b. *State of internet security: protecting small & medium businesses*. Boulder, CO: Webroot Software
- Websense Security Labs Research Team 2006. *First half 2006 security trends report*. San Diego, CA: Websense
- White M & Fisher C 2008. Assessing our knowledge of identity theft: the challenges to effective prevention and control efforts. *Criminal justice policy review* 19(1): 3–24
- Wilkins F 2006. Business in their sights. *Lawyers weekly* February: 17–19
- Yar M 2005. The novelty of 'cybercrime': an assessment in light of routine activity theory. *European journal of criminology* 2(4): 407–427

Appendix 1: Methodology



Sampling

The AIC obtained a business sampling frame from the ABS to provide a sample of Australian businesses from the ABS ABR. The ABR is a database of information provided by Australian businesses when they register for an Australian Business Number. A random, stratified sample of businesses was then extracted from the ABR. The sample was stratified by industry sector and business size (see Table 44). Businesses were selected from small (0–19 employees), medium (20–199 employees) and large (200 or more employees) businesses and from all 19 industries identified by ANZSIC (see ABS & Statistics New Zealand 2006). The ANZSIC industry sector classifications used in the survey were:

- agriculture, forestry and fishing
- mining
- manufacturing
- electricity, gas, water and waste services
- construction
- wholesale trade
- retail trade
- accommodation and food services
- transport, postal and warehousing
- information media and telecommunications

- financial and insurance services
- rental, hiring and real estate services
- professional, scientific and technical services
- administrative and support services
- public administration and safety
- education and training
- health care and social assistance
- arts and recreational services
- other services.

The target population for the survey was all Australian employing businesses, excluding defence force organisations, private households that employ staff, foreign diplomatic missions, and government and public sector businesses.

As shown in Table 44, the original sample comprised 20,040 businesses in total. Findings from the ABACUS pilot study (discussed below) indicated that a sample of this size would generate enough data to draw statistically significant conclusions about the business population of Australia.

The survey instrument

The questionnaire asked businesses to answer 38 questions relating to computer security incidents experienced by their business. In addition to

Table 44 Sample selections by industry sector and business size

	Small	Medium	Large	Total
Agriculture, forestry and fishing	945	77	33	1,055
Mining	865	150	40	1,055
Manufacturing	829	193	33	1,055
Electricity, gas, water and waste services	902	120	33	1,055
Construction	968	53	33	1,054
Wholesale trade	885	136	33	1,054
Retail trade	899	123	33	1,055
Accommodation and food services	795	226	33	1,054
Transport, postal and warehousing	945	77	33	1,055
Information media and telecommunications	892	130	33	1,055
Financial and insurance services	988	33	33	1,054
Rental, hiring and real estate services	932	90	33	1,055
Professional, scientific and technical services	962	60	33	1,055
Administrative and support services	879	143	33	1,055
Public administration and safety	829	193	33	1,055
Education and training	819	203	33	1,055
Health care and social assistance	912	110	33	1,055
Arts and recreational services	865	156	33	1,054
Other services	965	57	33	1,055
Total	17,076	2,330	634	20,040

Source: Challice (2008)

collecting basic demographic data, the survey asked questions about the number, type and cost of computer security incidents experienced by businesses, the consequences of these incidents and how businesses prevent and/or respond to these incidents.

The questionnaire was developed by the AIC with the assistance of a number of parties, including the Social Research Centre, and the Technical Advisory

Group and Business Advisory Group, which were established by the AIC to provide guidance on survey questions and other matters relating to the ABACUS study. Some of the questions were based on those contained in other similar surveys that have been conducted in Australia and overseas, in order to enable comparison among these jurisdictions.

The questionnaire was approved by the ABS Statistical Clearing House, whose role it is to ensure that surveys of businesses within Australia are necessary, well-designed and place minimal burden on respondents (see www.sch.abs.gov.au). Due to the large sample size, the acquisition of businesses' records from the ABS was also tabled in the Australian Parliament. The ABACUS project was granted AIC ethics approval under protocol no. 114 on 8 March 2007.

Participants were able to complete the questionnaire in one of three formats: hard copy, online or by CATI. These response options were provided to assist in maximising response rates for the survey. Seventy-eight percent of respondents completed hard copy questionnaires, 18 percent completed the questionnaire online and four percent completed the questionnaire via CATI.

The pilot study

A pilot ABACUS study was undertaken in April 2007. The primary objectives of the pilot study were:

- To test the proposed ABACUS survey instrument and methodology
- To gain an insight into the likely response rate of the main survey
- To collect data for preliminary analysis.

A total of 817 businesses were contacted and asked to complete the pilot questionnaire. Small, medium and large businesses from all Australian states and territories and from each of the 19 industry sectors used by ABACUS were contacted. Of these, 194 returned completed pilot questionnaires. The overall response rate for the pilot study was 24 percent.

Responses provided valuable information on a range of methodological issues, including ways to improve the survey instrument and maximise response rates. This information was used to inform the main ABACUS survey.

Main data collection

Data collection for the ABACUS study was undertaken by the SRC, a private research organisation based in Melbourne, Australia that specialises in providing research services to government agencies. The data collection took place during February, March and April of 2008. The SRC compiled data from all completed hard copy, CATI and online surveys and provided this data to the AIC for analysis. The following sections describe the process of the research study in detail.

Initial telephone call

An initial telephone call was made to the medium and large businesses in the sample to confirm their contact details and personalise the questionnaire to be mailed. The ABACUS pilot study findings suggested that personally addressing the mailed questionnaire, rather than sending generically addressed mail was likely to generate a higher number of responses. Small businesses were excluded from this process due to a lack of accurate telephone number details for small businesses. Of the 2,964 medium and large businesses in the sample, 16 were found to be either duplicate or overseas addresses. These business records were excluded from the sample. A further 491 could not be contacted by telephone due to these records containing inaccurate or incomplete telephone numbers.

Therefore, 2,457 medium and large businesses were contacted by an initial telephone call, comprising 83 percent of the initial medium and large business sample. Telephone calls were placed by SRC staff between 30 January 2008 and 25 February 2008.

Initial mail-out

Questionnaires were mailed to businesses in five batches between 1 February 2008 and 29 February 2008. Businesses that had been identified as duplicate, overseas or incomplete addresses, had declined to participate during the initial telephone

call or had been identified as out of scope during the initial telephone call were excluded from the initial questionnaire mail-out.

Businesses were posted a pack containing the 12-page questionnaire booklet, glossary, confidentiality statement, frequently asked questions sheet and reply paid envelope. The questionnaire booklet included an instruction sheet on the inside front cover and a covering letter on the outside front cover.

Telephone follow-up

A telephone call to all businesses that had not responded to the initial mail-out was planned to assist in maximising response rates. As stated above, however, the sample contained a considerable proportion of businesses without complete and accurate telephone numbers. A number of strategies were put into place to increase the proportion of the sample with a valid and unique telephone number. An attempt was made to reduce the number of business records with incomplete and/or inaccurate telephone numbers through the use of Macromatch, a Sensis process that provides or confirms businesses' telephone numbers where business names and addresses are provided. The Macromatch process is based on the online version of the Yellow Pages. A match was found for 4,197 (28%) of the 17,459 business records provided to Macromatch.

Follow-up telephone calls were made to the telephone number provided by businesses during the initial telephone call, the telephone number provided by Macromatch or the original, complete and unique telephone number provided in the initial sample. Following the initial mail-out, a total of 12,880 (72%) of the 17,694 non-responding businesses were able to be contacted by telephone at this stage of the research.

Businesses were also given the option to complete the survey over the telephone during this stage of the research. This only took place if the respondent had a full copy of the survey's Glossary to refer to at the time of the call.

Questionnaire re-mailing

A survey pack with a modified covering letter and revised due date was posted to remaining non-responding businesses between 4 April 2008 and 7 April 2008. A total of 9,660 businesses, including those that claimed not to have received a survey pack in the original mail-out, and non-responding businesses without a valid telephone number, were included in the re-mailing stage of the research. Survey packs were also re-mailed on an ad hoc basis in response to requests from members of the sample. In total, 10,267 survey packs were re-mailed to businesses to maximise response rates.

Response rates

In total, 4,000 ABACUS questionnaires were completed and returned from a sample of 13,941 in-scope businesses. After excluding out-of-scope businesses, the response rate for the survey overall was 29 percent. This varied by both business size and industry sector. Medium businesses had the highest response rate (32%), followed by small (28%) and then large businesses (27%). As shown in Table 45, response rates for industry sectors ranged from 20 percent for construction businesses to 37 percent for the agriculture, forestry and fishing sector.

Weighting of data

ABS population counts of industry sector and number of employees (business size) were used to develop the weighting matrix for the ABACUS sample data. Responses to questions one (industry sector) and two (number of employees) were used to allocate each questionnaire record to a cell for weighting. Where this information was not provided by the respondent, information from the original sample record was used.

Some respondents provided an answer for questions one and/or two that varied from information provided in the original sample record. In these instances, respondents were assigned to

Table 45 Response rate by industry sector and business size (percent)

	Small	Medium	Large	Overall
Agriculture, forestry and fishing	38	31	27	37
Mining	32	35	24	32
Manufacturing	29	35	38	31
Electricity, gas, water and waste services	29	35	23	30
Construction	19	41	10	20
Wholesale trade	29	31	17	29
Retail trade	26	25	25	26
Accommodation and food services	25	25	32	26
Transport, postal and warehousing	24	45	27	26
Information media and telecommunications	33	34	24	33
Financial and insurance services	29	39	15	29
Rental, hiring and real estate services	27	21	25	26
Professional, scientific and technical services	34	38	31	34
Administrative and support services	28	29	26	28
Public administration and safety	19	28	13	21
Education and training	32	36	33	33
Health care and social assistance	31	37	36	32
Arts and recreational services	26	27	53	28
Other services	24	27	37	25
Total	28	32	27	29

Source: Challice (2008)

a cell on the basis of the information they provided, so the information provided by respondents was taken to override existing information about industry sector and/or number of employees.

Data were weighted to represent the estimated total number of qualifying businesses in Australia according to the ABS.

Appendix 2: Glossary



Types of information technologies

Personal computers

A desktop computer, other than a laptop, designed for the use of business applications such as word processing, account keeping etc.

Laptops

A portable computer that is able to perform the same functions as a personal computer.

Smart phones

A mobile phone with personal computer-like functionality e.g. has the ability to carry out word processing applications, send and receive email, and access the internet.

Other wireless devices

Any device which operates, or the components of which operate, without the use of wires (i.e. via the use of electromagnetic waves).

Local area network

A computer network that encompasses a limited area such as a building or office.

Wide area network

A computer network that encompasses a large geographical area, such as a group of buildings

or separate offices, that are located in separate states or countries. Often comprising two or more local area networks.

Virtual private network

A network that is established via the use of public wires, such as telephone or broadband internet wires. These networks use encryption, digital certificates and other security tools to protect them against unauthorised access.

Types of computer security incidents

Insider abuse of access

An employee or person authorised to use a business's computer system abuses this access, such as downloading a large amount of data or accessing the internet for personal use against this business's IT policy.

Theft or loss of hardware

Hardware, such as laptops, Personal Digital Assistants or other devices, are lost or stolen and not recovered. Does not include hardware that is damaged or destroyed.

Virus or other malicious code

Software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse. May be either self-replicating or non self-replicating code (any statements and/or declarations that are written in a computer programming language) to change the way a computer operates without the consent or knowledge of the system owner or user. This includes all types of malware (malicious software) except spyware.

Spyware

Software designed to collect information from a computer secretly and send it elsewhere (e.g. key loggers) or change settings and interfere with the performance of a compromised computer.

Phishing

Assuming the identity of a legitimate organisation or website using forged email, fraudulent websites or other instant messaging communication forums such as MSN, to persuade others to provide information—usually personal financial, such as credit card numbers, account user names and passwords, social security numbers—for the purpose of using it to commit fraud.

Denial of service attack

An attack aimed at specific web sites by flooding the web server with repeated messages, depleting the system resources and denying access to legitimate users.

Sabotage of network or data

Intentional destruction of, or damage to, a computer network or to data stored on a network or stand alone computer.

Unauthorised network access

Obtaining access to a restricted computer network without providing adequate credentials such as log on name and password.

Theft or breach of proprietary or confidential information

The unauthorised access to, and/or, use, viewing, duplication, distribution or theft of, proprietary or confidential information. *Proprietary information* is information relating to or associated with a business's product, business or activities. It includes, but is not limited to, items such as trade secrets, research and development and financial information.

Incident involving the business's web application

Any malicious or destructive incident that involves a business's website. This may include placing unauthorised information on a website or preventing it from being used as intended.

Financial loss and financial cost

Financial cost and financial loss (as relating to either a specific computer security incident or all computer security incidents) should include all costs associated with the incident/s. These may include aspects such as the direct financial cost of the incident, staff costs in repairing the damage caused, loss of revenue due to the incident or any other cost that was a direct result of the incident. Do not include computer security measures implemented before or after the incident occurred.

Most significant incident

The most significant incident is the one that a business regards as causing the greatest negative effect or loss. Such incidents may include ones that caused the greatest financial loss, caused damage to a business's reputation and/or other negative effects.

Computer security incident outcomes

Corruption of hardware or software

Damage to computer hardware or software that renders it, in part or in whole, non-operational.

Corruption or loss of data

Damage to or interference with data that renders it, in part or in whole, non-operational.

Unavailability of service

Making the operations of a business either in part or in whole unavailable.

Website defacement

Damage caused to a public web site that limits or prevents its intended use.

Theft or loss of hardware

Refer definition for 'website defacement'.

Theft of business, confidential or proprietary information

Refer definition for 'website defacement'.

Non-critical operational losses

A disruption to a business that did not cause suspension or severe damage to a business's operations.

Non-critical financial losses

Loss of money or value to a business that did not cause a severe negative alteration to a business's financial state.

Harm to reputation

The reduction in confidence in a business or an increase in negative association with a business.

Critical operational losses

A disruption to a business that caused suspension or severe damage to a business's operations.

Critical financial loss

Loss of money or value to a business that caused severe negative alteration to a business's income or assets.

Loss of life

The death of a person who was, or was not, an employee of a business.

Computer security measures

Physical security

Using devices, such as locks, to secure computer hardware

Cryptographic and authentication tools

Cryptography is a means of scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called 'encryption'), then back again (known as 'decryption'). This enables securing of private information sent through public networks by encrypting it in a way that makes it unreadable to anyone except the person or persons holding the mathematical key or knowledge to decrypt the information.

Authentication software or hardware is designed to verify the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Digital certificates

Electronic documents signed by a trusted Certification Authority which identifies the key holder and the affiliated business entity, binds the key holder to a public/private key pair and contains other information required by the certificate profile (e.g. X.509, a commonly used ITU-T standard for public key infrastructure).

Biometrics

The use of a person's physical or behavioural characteristics as a form of identification and authentication. It includes, but is not limited to, retinal scans, finger/hand scans, keyboard ballistics, handwriting etc.

Smartcards

Smartcards, also known as chip cards, are plastic cards containing integrated circuits for information system access and identification and the holding of digital credentials and electronic value tokens.

Security tokens (other than smartcards)

Hardware devices designed to provide two-factor authentication by generating a one-time authentication key (in addition to a password or pin) which allows access to a network or system resources.

Password verification

The use of a password that is linked to an individual user account which allows access to network or system resources.

Single sign on

An identity management mechanism that allows account holders to authenticate themselves once when accessing inter-connected network and system resources.

Encryption of data

The process of scrambling or encoding of information to ensure that only the intended recipient (holding the corresponding decryption key or password) can read the information.

File integrity assessment tool

Software or hardware used to verify the integrity of the files' contents (i.e. to determine if a file has been modified).

Encrypting removable data storage devices

The process of scrambling or encoding of information on removable storage devices (such as USB drives or removable hard drives) to ensure that only the intended recipient (holding the corresponding decryption key or password) can read the information.

Anti-fraud and malware tools

Software or hardware designed to prevent fraud or malware (such as viruses) affecting a system or network.

Anti-spam filters

Software or hardware designed to identify, block and manage unsolicited email messages that are often used to commit fraud.

Anti-virus software

Software tools designed to identify, thwart and eliminate malicious code (i.e. virus, Trojans and worms) from a system, incoming email message etc.

Anti-spyware software

Software designed to detect and remove spyware from a system.

Anti-phishing software

Software designed to detect and prevent phishing attacks and the fraud that results from them. They can include Uniform Resource Locator (URL) blockers and fraud detection technologies.

Detection and monitoring tools

Software or hardware designed to monitor the use of a specific computer system or network.

Internet content filtering/image filtering or monitoring

Software or hardware designed for monitoring and limiting access to inappropriate information or data configured according to the organisation's security policy.

Intrusion detection system

Software applications designed to protect backbone services by detecting inappropriate, incorrect, or anomalous activities that cannot usually be detected by a conventional firewall.

Intrusion prevention system

Software or hardware designed to protect computers from exploitation by identifying and blocking potentially malicious activity in real time.

Security management tools

Software or hardware designed with the specific goal of managing and improving the security of computer systems and networks.

Endpoint security software

Endpoint security software (a suite of software and hardware) designed to work to prevent security breaches (e.g. data leakages) and to conform to defined enterprise and desktop security policies at endpoints. The latter can be an individual computing or storage device such as a client workstation for a network or personal computing device including laptops, desktops and Personal Digital Assistants.

Firewall

Software or hardware, designed for the protection of a network from unauthorised access, which permits, denies or provides proxy data connections configured according to the organisation's security policy.

Vulnerability management system

A process in which vulnerabilities are found and fixed and vulnerable systems are shielded. It includes configuration policy compliance, threat information, asset clarification, prioritisation and workflow.

Provisioning system

Provisioning systems allows the management of user accounts and user profiles that are linked to a person across an IT environment through a combination of user roles and business rules.

Security compliance tools

Software applications that enforce corporate and/or regulatory policies and standards.

Instant messaging security solutions

Software applications that enforce instant messaging (IM) usage policies such as the types of IM applications and IM attachments which are allowed.

Manual patch management

The process of controlling the deployment and maintenance of interim software releases (e.g. software updates) and security patches into production environments.

Automated patch management

The process of patch management, with minimal human intervention that enables automated analysis targeting and distribution of granular level patches (individual patches versus large service packs) and rapid quality-assurance testing.

Configuration management

The establishment of approved changes to the configuration of a computer system or network and the interrelation between system components.

Computer security policies

Staff related policies

Any computer security policy that is directed at the staff of a business.

Employee education and awareness program

Courses, seminars and other activities that are designed to increase the awareness and understanding of a business's employees of issues relating to computer security.

Segregation of duties

Where no individual has control over two or more phases of a transaction or operation within a business environment. Designed to prevent fraud.

System content monitoring

A system designed to specifically monitor information that is coming in and/or going out to/from a business's systems.

Wireless technology acceptable use policy

A policy that clearly defines what type of use is acceptable for a business's wireless technology i.e. acceptable download limits for wireless device.

IT acceptable use policies

A policy that clearly defines what type of use is acceptable for a business's information technology e.g. acceptable levels of personal use.

Mobile policies (such as mandatory encryption of data stored on mobile devices)

A policy that specifically relates to the use of mobile devices, such as Personal Digital Assistants. These types of policies can mandate what type of data may be stored on these devices or data that is required to be encrypted.

User access management policies

A policy that governs access rights (privileges) of individuals on a business's systems. These may also include the appropriate access rights of individuals to be recorded in an Access Control List.

Background checks

A policy that requires verification of information provided by employees of a business, such as checking for a criminal history prior to offering a candidate a position with a business.

Mandatory reporting of misuse/abuse of computer equipment

Policies that require a person to report misuse or abuse of computer equipment as soon as they become aware of it. This may include situations where an individual uses a business's system to download large amounts of personal data or access illegal or offensive content.

Documented standard operating procedures

A set of written instructions that governs the appropriate use of a business' information technologies.

Monitoring internet connections

A policy that governs how individual users' internet activity is monitored.

Account/password management policies

A policy that specifically relates to users' account and password information. These may include mandatory password lengths or frequency of password renewal.

Security testing policies/system penetration testing

A method to evaluate the security of a computer, system or network by simulating an electronic attack i.e. an attack by a hacker.

System audit policies

Policies mandating audits of a business's computers, including issues such as the frequency and type of audits carried out and details of those responsible for undertaking those audits. This is a measurable technical assessment of a network, system or application.

Risk assessment policies

Policies that govern the type and frequency of risk assessment of this business. Risk assessment is a process where the magnitude of potential loss and the probability it will occur are measured.

Data related policies

Any policies that relate to the handling, storage and security of data for this business.

Media backup procedures

Set policies and procedures that govern how the backup of data is recorded, stored and the frequency with which the backup occurs.

Management of removable computer media storage devices

Policies and procedures that govern if, how and when removable computer media devices can be used. For the purpose of this report, a removable computer media storage device is a device that connects either physically or wirelessly to another host or client device and allows the exchange of data between the two devices (e.g. USB drive or a removable hard drive, but excluding CDs, DVDs and diskettes).

Protection of electronic account information

Policies relating to the protection of customer, client or partner business information, such as credit card and personal details.

Incident response policies

Incident response policies include any policies that govern what responses are appropriate after a computer security incident has occurred.

Use of incident response team

Whether a business use consultants, not comprised of employees of this business, to investigate and respond to computer security incidents.

Business continuity policy

A policy or plan that allows a business to conduct its normal operations in the event of computer systems being non-operational or being severely impeded in their operation.

Forensic plan

A policy or set of guidelines that governs the preservation of digital evidence following a computer security incident.

Incident management procedures

A policy or set of guidelines that dictates a standard procedure for dealing with computer security incidents.

External business policies

Payment system supplier policies

Policies that a business is required to follow in order to use an external payment system provider (such as Paypal or credit card payments).

Other supplier determines policies

Policies that a business is required to follow in order to conduct business or use the services of another business.

Wireless security policies

Wireless security policies govern what types of security practices are used for the protection of data that is stored and transferred between wireless devices.

Secure placement of access points

Placement of wireless access points in a secure location, such as ceiling or on a high wall.

Name of network changed from default

Changing the default (original) name of the network to a unique name.

Encrypted signals

All signals sent by both wireless hosts and connecting devices are sent in an encrypted format.

Connections restricted to known devices only

Only hardware devices that have been 'set up' as part of the wireless network are able to access the network.

Wireless monitoring

Monitoring content that is sent and received by a wireless device.

Computer security and outsourcing evaluation methods

Security audit by internal staff

A measurable technical assessment of a network, system or application that is carried out by a staff member of a business.

Security audits by external businesses

A measurable technical assessment of a network, system or application that is carried out a person who is not a staff member of a business, e.g. a consultant.

Security compliance check

A form of assessment used to check a variety of security issues in terms of their compliance with a policy or guideline.

Automated tools

The use of software to monitor and report on the status of, and changes to, files and settings on individual systems, networks, servers etc.

Email monitoring software

Software that is designed to monitor the email activity of users.

Web activity monitoring software

Software that is designed to monitor the web activity (sites visited etc) of a specific user or users.

IT expenditure

IT expenditure includes all types of expenditure relating to a business's information technology.

These may include the cost of IT training, software and hardware and salaries for IT staff.

AIC Reports

Research and Public Policy Series 102

The Australian Business Assessment of Computer User Security (ABACUS) survey is a nationwide assessment of the prevalence and nature of computer security incidents experienced by Australian businesses. This report presents the findings of the survey which may be used by businesses in Australia to assess the effectiveness of their information technology security measures.

Australia's national research and
knowledge centre on crime and justice

www.aic.gov.au